GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-453B)

SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID 4.x

ABRIL 2015

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO 002-15-006-1

Fecha de Edición: abril de 2015
Raúl Siles (DinoSec) ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

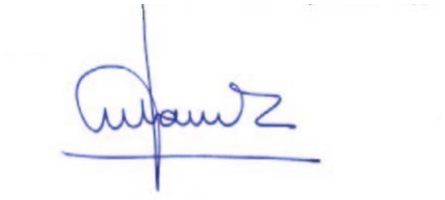
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Abril 2015



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El desarrollo de los dispositivos y comunicaciones móviles y de las tecnologías inalámbricas en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.

2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos, así como de los mecanismos de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).

3. Se considera dispositivo móvil aquél dispositivo de uso personal o profesional de reducido tamaño que permite la gestión de información y el acceso a redes de comunicaciones y servicios, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), tabletas (o *tablets*) y agendas electrónicas (PDAs), independientemente de sí disponen de teclado o pantalla táctil.

4. Pese a que los dispositivos móviles se utilizan para comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido una trascendencia relevante en los usuarios y en las organizaciones.

5. El presente documento realiza un análisis detallado de los mecanismos y la configuración de seguridad recomendados para uno de los principales sistemas operativos de dispositivos móviles utilizados en la actualidad, Android 4.x, en concreto hasta la versión 4.4.x, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

2. OBJETO

6. El propósito del presente documento es proporcionar una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basados en el sistema operativo Android versión 4.x (en adelante Android) [Ref.- 2], cuyo objetivo es proteger el propio dispositivo móvil, sus comunicaciones y la información y datos que gestiona y almacena.

7. La presente guía proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad generales descritas en la guía principal de esta misma serie, que presenta la información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.

8. La serie CCN-STIC-450, "Seguridad de dispositivos móviles", se ha estructurado en dos niveles: una guía genérica centrada en al análisis de seguridad de dispositivos móviles (CCN-STIC-450), complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día. Por este motivo, antes de la lectura y aplicación de la presente guía, asociada a un sistema operativo (y versión concreta del mismo), se recomienda la lectura de la guía general de seguridad:

   - CCN-STIC-450 - Seguridad de dispositivos móviles

9. La presente guía está basada en la versión previa de la misma guía "*Seguridad de dispositivos móviles: Android*", centrada en la versión 2.x de Android y publicada en el año 2013 [Ref.- 130].

10. Adicionalmente, se recomienda la lectura de las guías de esta misma serie asociadas a otros sistemas operativos y versiones de plataformas móviles, en caso de ser necesaria su aplicación en otros terminales, y a la gestión empresarial de dispositivos móviles (MDM):

    - CCN-STIC-451 - Seguridad de dispositivos móviles: Windows Mobile 6.1
    - CCN-STIC-452 - Seguridad de dispositivos móviles: Windows Mobile 6.5
    - CCN-STIC-453 - Seguridad de dispositivos móviles: Android 2.x
    - CCN-STIC-454 - Seguridad de dispositivos móviles: iPad (iOS 7.x)
    - CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone (iOS 7.x)
    - CCN-STIC-457 - Gestión de dispositivos móviles: MDM (*Mobile Device Management*) [Ref.- 131]

Nota: esta serie de guías están diseñadas considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades y funcionalidad disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

3. ALCANCE

11. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los dispositivos móviles ya existentes o futuros bajo su responsabilidad.

4. ENTORNO DE APLICACIÓN DE ESTA GUÍA

12. Android es un entorno software de código abierto (*open-source*) basado en Linux (originalmente en el kernel 2.6.x) y diseñado para dispositivos móviles que incluye el sistema operativo y el kernel, un conjunto de librerías (y APIs asociadas), el entorno de ejecución (Dalvik VM y ART, Android RunTime) y el entorno de desarrollo para las aplicaciones móviles (de aquí en adelante referenciadas como apps, indistintamente, y por abreviar), junto a un conjunto de aplicaciones móviles (o apps) disponibles por defecto [Ref.- 11] [1] (ver siguiente imagen).

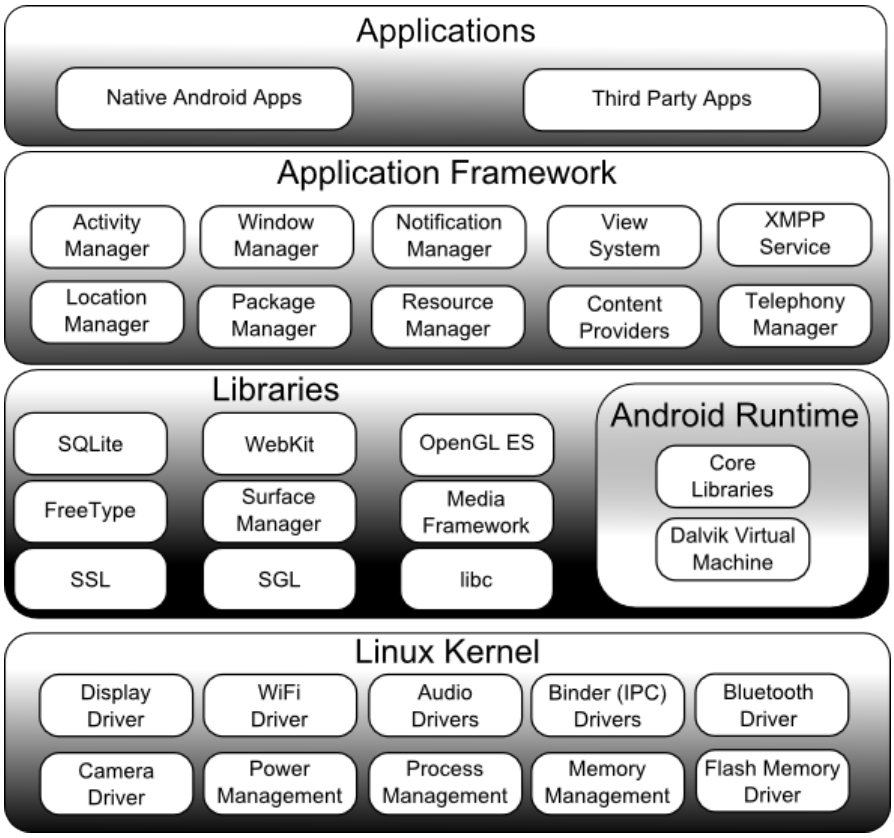
13. Inicialmente desarrollado por Android Inc., fue adquirido por Google en el año 2005, colaborando en su desarrollo la Open Handset Alliance (OHA), y encargándose de su mantenimiento el Android Open Source Project (AOSP) [Ref.- 81]. La primera versión comercial, Android 1.0, fue publicada en septiembre de 2008 [Ref.- 128].

14. La evolución de las versiones posteriores de Android (desde las versiones 2.x a las 4.x) ha conllevado notables modificaciones sobre el kernel de Linux estándar, y pese a seguir empleándose versiones y referencias al kernel de Linux 3.x, en los años 2010 y 2011 cada vez el entorno Android distaba más de un entorno Linux tradicional. Sin embargo, ambos proyectos, Android y Linux, volvieron a reunificarse en la versión 3.3 del kernel[2].

[1] Imagen: http://www.techotopia.com/index.php/Image:Android_architecture2.png
[2] http://www.zdnet.com/article/android-and-linux-re-merge-into-one-operating-system/

15. Las versiones de Android (desde la versión 1.5) emplean nombres en clave correspondientes a nombres de postres y dulces en inglés, ordenados alfabéticamente. A continuación se muestra el listado de versiones de Android conocidas en el momento de elaboración de la presente guía:

    - Alpha (1.0)
    - Beta (1.1)
    - Cupcake (1.5)
    - Donut (1.6)
    - Eclair (2.0–2.1)
    - Froyo (2.2–2.2.3)
    - Gingerbread (2.3–2.3.7)
    - Honeycomb (3.0–3.2.6)
    - Ice Cream Sandwich (4.0–4.0.4)
    - Jelly Bean (4.1–4.3.1)
    - KitKat (4.4–4.4.4)
    - Lollipop (5.0)



16. El primer dispositivo móvil Google Nexus, basado en Android 2.1, fue el *smartphone* Nexus One (dispositivo empleado en la versión previa de la presente guía y desarrollado por Google y HTC), que se empezó a comercializar en enero de 2010. Posteriormente, en

mayo de 2010, fue actualizado a la versión Android 2.2 y comercializado como el primer dispositivo móvil con esta nueva versión de Android.

17. Android versión 2.2 (con nombre en clave "Froyo") fue la versión por defecto incluida en numerosos dispositivos móviles disponibles en el mercado durante los años 2010 y 2011, complementando versiones previas, como la versión 2.0/2.1 de Android ("Eclair"), 1.6 ("Donut") y 1.5 ("Cupcake") [Ref.- 128].

18. La versión 2.2 (analizada en la versión previa de la presente guía) añadió, entre otras, mejoras de rendimiento, la versión V8 del motor de JavaScript Chrome, la posibilidad de actuar como hotspot Wi-Fi para compartir la conexión de datos de telefonía móvil con otros dispositivos, y soporte para Adobe Flash en el navegador web.

19. Android anunció una actualización en diciembre de 2010 asociada a la versión 2.3 ("Gingerbread") [Ref.- 9], que añadía mejoras en el interfaz de usuario, el teclado táctil y las capacidades de copiar y pegar datos, así como soporte para SIP (voz sobre IP, VoIP) y NFC (Near Field Communication - con capacidades extras añadidas en la versión 2.3.3 [Ref.- 10]). El primer dispositivo móvil basado en Android 2.3 fue el *smartphone* Nexus S (desarrollado por Google y Samsung), comercializado en la misma fecha de lanzamiento que Android 2.3.

20. La versión 3.0 de Android ("Honeycomb") fue diseñada para dispositivos en formato tableta (o *tablets*), con pantalla de mayor tamaño y mayor capacidad de procesamiento (tanto del procesador principal como gráfico). Esta versión añadió la posibilidad de aplicar un cifrado completo a los datos almacenados en el dispositivo móvil [Ref.- 82]. El primer dispositivo móvil basado en Android 3.0, la tableta o *tablet* Motorola Xoom, se empezó a comercializar en el mercado en febrero de 2011.

21. Posteriormente se publicaron las versiones 3.1 y 3.2 en mayo y julio de 2011 respectivamente. La versión 3.1 añadió soporte para más dispositivos de entrada y conexión USB para la transferencia de ficheros, mientras que la versión 3.2 añadió soporte para tarjetas de memoria SD y mejoras en la gestión de la pantalla y de distintas resoluciones gráficas.

22. La versión 4.0 de Android ("Ice Cream Sandwich", ICS), basada en el kernel 3.0.1 de Linux, fue anunciada en octubre de 2011 y proporcionó gran parte de la funcionalidad existente en "Honeycomb" a los *smartphones* (no únicamente a *tablets*), añadiendo un gran número de funcionalidades y cambios en el interfaz de usuario, como por ejemplo mejoras en las capacidades multitarea, nuevas funcionalidades en la pantalla de desbloqueo (como el acceso directo a la cámara o el acceso al centro de notificaciones), control de acceso mediante reconocimiento facial utilizando la cámara frontal, control y monitorización del tráfico de red y datos (redes móviles y/o Wi-Fi), la posibilidad de compartir información mediante NFC (y Android Beam), soporte para Wi-Fi Direct (o Wi-Fi Peer-to-Peer, "P2P"), soporte para el perfil Bluetooth HDP (*Health Device Profile*) y para la conexión a sensores y dispositivos médicos y de salud inalámbricos, y nuevas capacidades de gestión y almacenamiento de credenciales y certificados digitales (keychain API [Ref.- 185]), entre otros. El primer dispositivo móvil basado en Android 4.0, el *smartphone* Galaxy Nexus (desarrollado por Google y Samsung), se empezó a comercializar en noviembre de 2011.

23. Android 4.0 implementó ASLR (*Address Space Layout Randomization*) para proteger tanto los componentes del sistema como las aplicaciones móviles (apps) de terceros frente a la explotación de vulnerabilidades en la gestión de memoria. Adicionalmente, Android 4.0 incorporó el *Android VPN Framework* (AVF, o VPN API), que añade por defecto un cliente VPN con soporte para L2TP e IPSec. En versiones previas de Android el uso de

software de conexión a redes VPN, en algunos escenarios, requería disponer de un dispositivo móvil Android *rooted* (o *rooteado*).

24. Desde el punto de vista de la gestión, se añadieron controles para poder deshabilitar remotamente la(s) cámara(s) del dispositivo móvil mediante las soluciones de gestión empresarial de dispositivos móviles o MDM (*Mobile Device Manager*) y mediante el uso de la app de gestión de Google asociada (de tipo *Device Policy Manager*) en Android.

25. La versión 4.1 de Android ("Jelly Bean", JB) fue anunciada en la conferencia Google I/O en junio de 2012, centrada en mejorar la funcionalidad y rendimiento del interfaz de usuario, y con nuevas capacidades como las transferencias de datos mediante Bluetooth vía Android Beam (adicionalmente a las basadas en NFC), el descubrimiento de servicios a través de Wi-Fi Direct (o Wi-Fi "P2P"), o el descubrimiento de servicios a través de *multicast* DNS en redes Wi-Fi (Wi-Fi NDS, *Network Service Discovery*). El primer dispositivo móvil basado en Android 4.1, la tableta o *tablet* Nexus 7 (desarrollada por Google y Asus), se empezó a comercializar en julio de 2012.

26. Adicionalmente la versión 4.1 de Android añadió soporte para GCM (*Google Cloud Messaging*), un servicio que permite el envío de mensajes y notificaciones *push* a los usuarios de apps específicas por parte de sus desarrolladores desde sus servidores a través de Google. Estas capacidades pueden ser también empleadas, por ejemplo, por las soluciones empresariales de gestión de dispositivos móviles (MDM).

27. Asimismo, Android 4.1 añadió múltiples capacidades a Google Play, como funcionalidad para proteger las apps de pago y sus contenidos mediante cifrado, empleando una contraseña específica para cada dispositivo móvil, antes de ser distribuidas y almacenadas desde la tienda o mercado oficial de apps de Google. Los nuevos servicios de Google Play también permiten integrar las capacidades de autentificación asociadas a la cuenta de usuario de Google en las apps de Android, así como integrarlas con Google+. Con el objetivo de mejorar y optimizar la distribución de nuevas actualizaciones de las apps, las actualizaciones de apps inteligentes (*Smart App Updates*) permiten enviar a los dispositivos móviles Android únicamente los elementos de la app que han sido actualizados, en lugar del paquete de Android (o APK) completo de la app.

28. La versión 4.2 de Android (también denominada "Jelly Bean"), basada en el kernel 3.4.0 de Linux, fue anunciada en octubre de 2012[3], e introducía nuevas capacidades en la pantalla de desbloqueo (como el soporte para complementos, *widgets*), soporte para múltiples cuentas o perfiles de usuario (sólo para tabletas), la reimplementación de la pila NFC y de la pila Bluetooth (pasando de BlueZ a BlueDroid, esta última desarrollada por Google y Broadcom), soporte para pantallas externas (incluso a través de Wi-Fi, mediante *Wi-Fi Display*), la ocultación de las opciones de desarrollo por defecto, debiendo activarse manualmente, y optimizaciones en el entorno de ejecución Dalvik VM. Los primeros dispositivos móviles basados en Android 4.2 fueron el Nexus 4 (*smartphone* desarrollado por Google y LG) y la Nexus 10 (tableta desarrollada por Google y Samsung), ambos comercializados en noviembre de 2012.

29. La versión 4.2 añadió notables mejoras de seguridad [Ref.- 83] [Ref.- 138], destacando:

    - *Always-on* VPN, para permitir que las apps únicamente generen tráfico de red si existe una conexión VPN activa y proteger así el envío de datos no cifrados a través

[3] Android 4.2 fue anunciada a través de una nota de prensa debido al huracán Sandy.

de otras redes que podrían acceder a la información transmitida (ej. directamente a través de Internet); ver apartado "5.17.6. Redes VPN".

- Generación de notificaciones, y confirmación por parte del usuario, antes de realizar el envío de mensajes SMS *premium* (con coste adicional).
- Verificación de apps, funcionalidad que permite analizar las aplicaciones móviles (apps) antes de su instalación para detectar si disponen de código o funcionalidades dañinas conocidas (*malware*).
- La librería principal con soporte para SSL/TLS añadió soporte para *certificate pinning* [Ref.- 76], permitiendo disponer de un mayor control sobre el certificado digital empleado por una app o dominio concreto, y evitando problemas de seguridad asociados a las autoridades certificadoras (CAs, *Certificate Authorities*).
- Organización de los permisos de las apps en grupos, lo que simplifica su aprobación por parte del usuario estándar, pero limita la granularidad en su análisis y en la autorización por parte de usuarios avanzados.
- El demonio *installd* encargado de la instalación de apps no ejecuta con permisos de root (o superusuario), limitando así la explotación de potenciales vulnerabilidades sobre este componente.
- Los scripts de arranque (*init scripts*) aplican la semántica basada en la directiva O_NOFOLLOW para prevenir ataques mediante enlaces (o *links*) simbólicos.
- Por defecto, las apps que hacen uso de la API 17 o superior no exportan sus proveedores de contenidos (ContentProviders), reduciendo así su exposición frente a ataques.
- Por defecto, las apps que hacen uso de la API 17 o superior y que utilizan WebViews no permiten el acceso directo al método "addJavascriptInterface()", limitando la ejecución remota de código en la interacción entre JavaScript y Java, y reduciendo así su exposición frente a ataques.
- Mejoras en la implementación por defecto para la generación de números aleatorios (SecureRandom) y RSA pasa a hacer uso de OpenSSL (1.0.1), con soporte para TLS v1.1 y v1.2.
- Múltiples actualizaciones de seguridad de librerías, como por ejemplo WebKit, libpng, OpenSSL, y LibXML.

30. Adicionalmente, la versión Android 4.2 proporcionó una nueva funcionalidad para establecer conexiones USB seguras con un ordenador (concretamente desde la versión Android 4.2.2 y posteriores), autentificando las conexiones ADB mediante un par de claves RSA, y solucionó la vulnerabilidad Master Key (teóricamente desde Android 4.2.2, aunque la versión concreta depende del fabricante del dispositivo móvil).
31. La versión 4.3 de Android (también denominada "Jelly Bean"), fue liberada en julio de 2013, con soporte para Bluetooth Smart (o BLE, Bluetooth Low Energy - disponible inicialmente en los modelos Nexus 4 y Nexus 7 2013), acceso restringido para nuevos perfiles de usuario, la disponibilidad temporal de "App Ops" (un sistema granular de

control de permisos para las aplicaciones móviles, oculto por defecto[4]), optimizaciones en el cálculo de la localización vía hardware en lugar de software (*hardware geofencing*) y soporte para la obtención de información de redes Wi-Fi cercanas para los servicios de localización, incluso cuando el interfaz Wi-Fi está apagado. La mayoría de dispositivos móviles Nexus obtuvieron la actualización 4.3 a la semana de su publicación, y el primer dispositivo móvil en ser comercializado directamente con Android 4.3 fue la segunda generación de la *tablet* Nexus 7, conocida como Nexus 7 2013 (también desarrollada por Google y Asus), en julio de 2013.

32. La versión 4.3 añadió notables mejoras de seguridad [Ref.- 83] [Ref.- 138], destacando:

- Las apps pueden configurar las credenciales de redes Wi-Fi WPA(2)-Empresariales que necesiten, pudiendo emplear múltiples métodos de autentificación basados en el estándar EAP (Extensible Authentication Protocol).
- La API de keychain dispone de nuevas capacidades para establecer que un conjunto de credenciales no puede ser exportado fuera del dispositivo móvil, es decir, se vinculan al hardware o dispositivo móvil concreto. Asimismo, las apps disponen de capacidades para almacenar credenciales en un *keystore* privado que no esté accesible a otras apps, y estas credenciales pueden ser añadidas sin interacción del usuario, siendo posible definir que tampoco puedan ser exportadas.
- La partición de sistema ("/system") en Android 4.3 es montada con restricciones mediante el parámetro o flag *nosuid*, y los procesos derivados de zygote no disponen de capacidades para ejecutar programas SUID, limitando por tanto la ejecución de programas con *setuid* o *setgid* por parte de las apps (por ejemplo, con privilegios de root o superusuario), y evitando así la explotación de ciertas vulnerabilidades previamente conocidas. Adicionalmente se eliminaron numerosos programas *setuid* o *setgid*.
- Tanto zygote como ADB reducen sus capacidades antes de ejecutar apps, evitando así que las apps ejecutadas tanto desde el propio Android como desde una *shell* (a través de ADB) no dispongan de capacidades privilegiadas. Adicionalmente zygote evita que se añadan nuevas capacidades antes de ejecutar código por parte de las apps, evitando la elevación de privilegios vía "execve".
- Utilización de las capacidades FORTIFY_SOURCE por parte de las librerías y aplicaciones del sistema para prevenir la explotación de vulnerabilidades de *strings* no terminados adecuadamente o de corrupción de memoria, junto a otras protecciones en la reubicación de código (*relocation*) para binarios enlazados estáticamente y en el propio código de Android.
- Soporte para MAC (*Mandatory Access Control*, frente a *Discretionary Access Control*, DAC) en Android a través de SELinux (Security-Enhanced Linux) [Ref.- 140] y la definición asociada de políticas de seguridad. En Android 4.3 se hace uso de SELinux en modo permisivo o *permissive mode*, donde únicamente las acciones no legítimas son registradas por el kernel, pero no bloqueadas [Ref.- 139] [Ref.- 140].

[4] Este sistema granular de control de permisos para las aplicaciones móviles que puede ser usado tras su instalación, fue eliminado en una versión posterior de Android por Google, concretamente en la versión 4.4.2.

- Las capacidades MAC (*Mandatory Access Control*) de SELinux en Android se pueden emplear en todos los procesos, tanto los asociados a las apps como los procesos de sistema que ejecutan como root o system (aplicando el modelo de permisos basado en *Linux capabilities*), dependiendo de la versión de Android.

33. La versión 4.4 de Android ("KitKat", KK [Ref.- 146]) fue anunciada en septiembre de 2013, optimizada específicamente para ejecutar en dispositivos más básicos con capacidades reducidas, incluso con tan sólo 512 MB de memoria RAM (o incluso menos[5]; *Project Svelte*[6]). Adicionalmente, esta versión añadió capacidades de impresión inalámbricas, soporte para emulación de *host* en NFC (HCE, *Host Card Emulation*), permitiendo que las apps de un dispositivo móvil lean y emulen *smartcards* NFC (como las empleadas como medio de pago en las tarjetas EMV), incorporó nuevos perfiles Bluetooth (*Bluetooth HID over GATT* (HOGP), MAP (*Message Access Profile*) y extensiones para AVRCP), soporte para *Wi-Fi Tunneled Direct Link Setup* (TDLS), añadió una implementación nueva de WebView basada en Chromium, añadió también la certificación *Wi-Fi Display Specification* haciendo compatibles con Miracast a los dispositivos móviles Android 4.4 (como por ejemplo el modelo Nexus 5), e introdujo el nuevo entorno de ejecución ART (Android RunTime) como futuro sustituto de Dalvik VM, pero todavía de manera experimental y no habilitado por defecto. El primer dispositivo móvil basado en Android 4.4 fue el *smartphone* Nexus 5 (desarrollado por Google y LG), comercializado en octubre de 2013. Posteriormente, la actualización de Android 4.4 (KitKat) se extendió a otros dispositivos móviles de Google, como el Nexus 4, Nexus 7 o Nexus 10, y de otros fabricantes.

Nota: Android 4.4 (KitKat) introdujo soporte nativo para (Google) Cloud Print[7], un servicio que permite imprimir desde cualquier dispositivo móvil Android (y otros dispositivos y ordenadores), y desde cualquier lugar, en cualquier impresora conectada a Cloud Print, y cuya configuración está disponible bajo el menú "Ajustes [Sistema] - Impresión". Las versiones previas de Android pueden utilizar la app Cloud Print[8], disponible en Google Play, para hacer uso de este servicio. Se recomienda deshabilitar las capacidades de impresión de Android si no se está haciendo uso de ellas (habilitadas por defecto). El análisis de seguridad de Cloud Print queda fuera del alcance de la presente guía.

Igualmente, Android dispone de capacidades para extender la funcionalidad del teclado existente por defecto mediante la instalación de apps de teclado de terceros (IME, Input Method Editor). Debido a que el teclado gestiona la mayoría de la entrada de datos del usuario, incluyendo contraseñas, un teclado malicioso podría registrar todo lo que teclea el usuario en un fichero local, e incluso enviarlo a un servidor remoto a través de Internet. Por este motivo, debe prestarse especial atención a los teclados acualmente instalados, disponibles desde el menú "Ajustes [Personal] - Idioma e introducción de texto [Teclado y métodos de introducción]", eliminando aquellos en los que no se confie, y tomar precauciones a la hora de instalar nuevos teclados [Ref.- 190]. El análisis de seguridad de teclados adicionales en Android queda fuera del alcance de la presente guía.

34. Las subversiones de la versión 4.4 añadieron capacidades destacables, como una mejor compatibilidad con las aplicaciones móviles para ART en 4.4.1, la eliminación del sistema

[5] El valor mínimo de RAM necesario para ejecutar Android se supone que es de 340MB.
[6] http://android-developers.blogspot.com.es/2013/10/android-44-kitkat-and-updated-developer.html
[7] http://www.google.com/cloudprint/learn/index.html
[8] https://play.google.com/store/apps/details?id=com.google.android.apps.cloudprint&hl=es

de control de permisos "App Ops" en 4.4.2 (añadido en Android 4.3) o cambios para solucionar la vulnerabilidad de Heartbleed de OpenSSL en 4.4.3.

35. La versión 4.4 añadió notables mejoras de seguridad [Ref.- 83] [Ref.- 138], destacando:

    - Granularidad para configurar redes VPN por usuario en dispositivos multiusuario, permitiendo a un usuario redirigir todo su tráfico a través de una red VPN sin afectar a otros usuarios.
    - Soporte para las capacidades FORTIFY_SOURCE de nivel 2, y su aplicación a todo el código fuente de Android, que ha sido compilado con estas protecciones.
    - Soporte para dos nuevos algoritmos criptográficos: *Elliptic Curve Digital Signature Algorithm* (ECDSA y DSA) para el almacenamiento de credenciales en los proveedores *keystore* y la utilización de firmas digitales, y soporte para la función de derivación de claves scrypt a la hora de proteger las claves empleadas en el cifrado completo del dispositivo móvil.
    - Notificaciones de seguridad avisando al usuario cuando se añaden certificados digitales al repositorio del dispositivo móvil.
    - Capacidades de protección adicionales empleando *certificate pinning* para detectar y prevenir el uso de certificados fraudulentos en comunicaciones SSL/TLS asociadas a los servicios de Google.
    - Mejoras para eliminar las vulnerabilidades PileUp o Fake ID (existente desde Android 2.1).
    - En Android 4.4 se hace uso de SELinux en modo obligatorio o *enforcing mode* parcialmente, es decir, sólo para un conjunto crítico de procesos o dominios de sistema (installd, netd, vold y zygote), en el que todas las acciones no legítimas son bloqueadas y registradas por el kernel [Ref.- 139] [Ref.- 140]. Para el resto de procesos o dominios, SELinux en Android 4.4 sigue actuando en modo permisivo, como en el caso de Android 4.3.

36. La versión 4.4.4 de Android soluciona específicamente una vulnerabilidad de seguridad asociada a OpenSSL que permitía la realización de ataques MitM (Man-in-the-Middle) tanto sobre clientes como sobre servidores, con el identificador CVE-2014-0224[9], y que permite forzar el uso de una clave maestra débil (vacía) en ciertos escenarios de comunicación entre versiones de OpenSSL, conocida como la vulnerabilidad de "inyección CCS (ChangeCipherSpec)" [Ref.- 136] [Ref.- 137][10].

37. Posteriormente, en julio de 2014, y asociada a la API 20 (en lugar de la API 19 de la versión 4.4 de Android estándar) se anunció la versión 4.4W (o 4.4WE) de Android, con extensiones para dispositivos personales (Wearable Extensions, WE) [Ref.- 133].

Nota: el resumen previo de las diferentes versiones de Android no hace referencia específica a las subversiones, como por ejemplo las versiones 4.0.4, 4.3.1 o 4.4.4, salvo que se haya considerado relevante destacar alguna funcionalidad concreta de alguna subversión.

[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224

[10] Esta vulnerabilidad se solucionó adicionalmente a través de los servicios de Google Play para otras versiones de Android.

Como referencia, se han incluido referencias a los dispositivos móviles de la gama Google Nexus[11] asociados a cada versión principal de Android.

38. La versión 5.0 de Android ("Lollipop") ha sido liberada en noviembre de 2014, con notables mejoras incluyendo el nuevo interfaz gráfico de usuario basado en *Material Design*, haciendo uso de ART (Android RunTime) por defecto, con soporte para CPUs de 64 bits, nuevas capacidades asociadas a la pantalla de desbloqueo y el centro de notificaciones, etc. Los primeros dispositivos móviles basados en Android 5 han sido el *smartphone* Nexus 6 (desarrollado por Google y Motorola Mobility) y la *tablet* Nexus 9 (desarrollada por Google y HTC), ambos comercializados en noviembre de 2014.
39. En Android 5.0 se hace uso de SELinux en modo obligatorio o *enforcing mode* globalmente o completo (*full enforcement*), es decir, tanto para el conjunto crítico de procesos de sistema (ya protegidos en Android 4.4), como para el resto de procesos (con más de 60 dominios) [Ref.- 139] [Ref.- 140].
40. Las principales diferencias y novedades de cada una de las versiones de la plataforma Android están disponibles en la página web para desarrolladores de Android: 2.2, 2.3, 3.0, 4.0 (Ice Cream Sandwich, ICS), 4.1, 4.2 y 4.3 (Jelly Bean, JB), 4.4 (KitKat) y 5.0 (Lollipop) [Ref.- 83].
41. Los contenidos de esta guía aplican a dispositivos móviles basados en Android en castellano: "Español (España)". El idioma puede ser seleccionado desde el menú "Ajustes [Personal] - Idioma e introducción de texto - Idioma".
42. La guía ha sido probada y verificada con la versión 4.4.4 del sistema operativo Android.

Nota: la información general del dispositivo móvil está disponible bajo la opción "Ajustes [Sistema] - Información del teléfono", y en concreto, la información de la versión del sistema operativo se encuentra bajo la sección "Versión de Android".

43. Las operaciones que requieren del uso de un ordenador han sido llevadas a cabo mediante Windows 7 Home Premium 64-bits (Service Pack 1) en inglés.

Nota: para la elaboración de la guía se ha empleado la versión de Windows 7 en inglés en el ordenador utilizado para la conexión y sincronización con el dispositivo móvil, con el objetivo de ejemplificar la compatibilidad de idiomas entre el terminal y el ordenador. La simplicidad de las funciones realizadas a través del ordenador, pese a utilizarse otro idioma, no debería dificultar la comprensión de la presente guía.

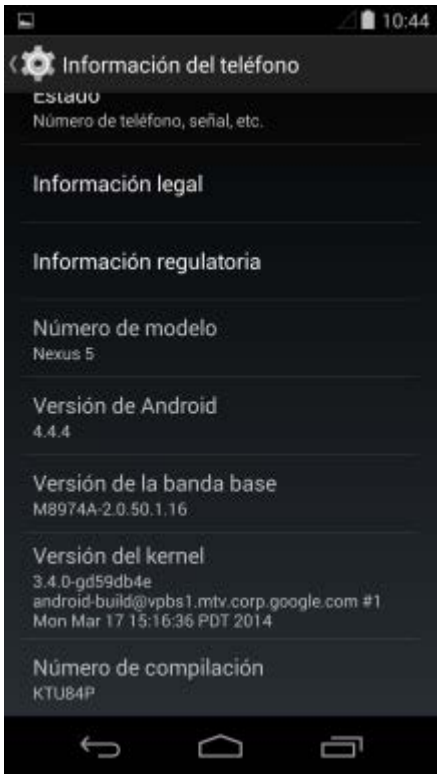
Nota: la presente guía emplea el término "ordenador" para referenciar al equipo portátil o de sobremesa (o escritorio) empleado para la sincronización, gestión y tareas de administración, depuración y desarrollo sobre el dispositivo móvil.

44. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características:
    - Dispositivo móvil Google Nexus 5 (fabricado por LG, modelo LG-D821) [Ref.- 3]:
        - Versión de Android [12]: 4.4.4
        - Versión de banda base: (ver imagen inferior): M8974A-2.0.50.1.16

[11] http://en.wikipedia.org/wiki/Google_Nexus y http://www.google.es/nexus/
[12] La versión disponible por defecto en el momento de adquisición del terminal empleado era Android 4.4.2.

- Versión de kernel: (ver imagen inferior): 3.4.0-gd59db4e ... Mar 17 ... 2014
- Número de compilación: KTU84P

Nota: el dispositivo móvil empleado es un terminal libre, es decir, no asociado a ningún operador de telefonía móvil, con el objetivo de analizar las características y valores por defecto de Android sin verse afectadas por las posibles modificaciones y personalizaciones llevadas a cabo por los operadores de telefonía.



Nota: la guía ha sido diseñada (y aplicada) para dispositivos móviles estándar basados en Android en los que no se ha llevado a cabo el proceso de *rooting*. Este proceso permite al usuario disponer de control completo del dispositivo móvil y acceder al mismo como root, superusuario, o usuario privilegiado, y en concreto, al subsistema Linux subyacente en Android, eliminando así los controles y/o restricciones establecidos por la plataforma Android estándar, los fabricantes y/o los operadores de telefonía móvil asociados al dispositivo móvil.

Las apps disponibles para los dispositivos móviles Android, por defecto, no disponen de permisos de escritura en ciertas zonas del sistema de ficheros, no pudiendo reemplazar el sistema operativo, ni de privilegios para hacer uso de capacidades específicas, como reiniciar el dispositivo móvil, modificar el uso de los LEDs hardware, capturar la pantalla del dispositivo móvil o eliminar aplicaciones móviles instaladas por algunos operadores de telefonía móvil. El proceso de *rooting* es utilizado por usuarios avanzados para acceder a estas funcionalidades de bajo nivel.

Los dispositivos móviles Android *rooted* ignoran el modelo de seguridad descrito a lo largo de la presente guía, ya que todas las aplicaciones que sean instaladas podrán disponer de los máximos privilegios en el dispositivo (root), exponiendo potencialmente a los usuarios a código dañino que podría tomar control completo del terminal. Android no requiere llevar a

cabo el proceso de *rooting* para permitir la instalación de apps de terceros no oficiales, es decir, no distribuidas a través de Google Play, tal como sucede en otras plataformas de dispositivos móviles, como iOS, donde es necesario realizar el proceso de *jailbreak* (equivalente a *rooting*) para poder instalar ese tipo de apps no oficiales.

Las particularidades del proceso de actualización en Android (ver apartado "5.1. Actualización del sistema operativo: Android"), con largos periodos de tiempo hasta que una nueva actualización está disponible para algunos usuarios, es uno de los motivos que incentiva a muchos usuarios a realizar el proceso de *rooting* para así poder instalar la última versión de Android en su dispositivo móvil.

Nota: debe tenerse en cuenta que se pueden presentar diferencias en la apariencia de las capturas de pantalla utilizadas a lo largo de la presente guía y la pantalla de otros dispositivos móviles basados en Android, debido al modelo, fabricante o versión concreta del SO.

Asimismo, algunas de las funcionalidades disponibles en Android pudieran ser propias de un fabricante de dispositivos móviles determinado, por lo que las recomendaciones de seguridad asociadas no aplicarían a otros dispositivos móviles basados en Android. Se recomienda llevar a cabo un análisis de seguridad similar al mostrado para estas funcionalidades adicionales añadidas por los fabricantes con el objetivo de determinar las recomendaciones a aplicar en dispositivos móviles de otros fabricantes y en sus aplicaciones propietarias.

45. La versión 4.4.4 de Android para el dispositivo móvil empleado para la elaboración de la presente guía (Nexus 5) estuvo disponible como actualización parcial OTA (Over-the-Air), con sólo 2,5MB de tamaño desde la versión 4.4.3 de Android, y complementariamente a la imagen de fábrica completa de esta versión de sistema operativo [13], desde finales de junio de 2014 [Ref.- 58] (ver apartado "5.1. Actualización del sistema operativo: Android").
46. Se recomienda siempre recabar e inventariar la información de versiones, tanto hardware como software, de los dispositivos móviles a proteger, con el objetivo de disponer de toda la información necesaria a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones y medidas de seguridad.
47. Debe prestarse atención al contrato de telefonía, y en concreto de datos, asociado a la tarjeta SIM (Subscriber Identity Module) empleada en el dispositivo móvil Android. La ausencia de capacidades de comunicación de datos es notificada al usuario en función de las apps que requieren disponer de las mismas.
48. Igualmente, debe prestarse especial atención al tipo de dispositivo móvil (marca y modelo) donde se desea aplicar la guía ya que la relación de los elementos descritos o referenciados en la presente guía (interfaz de usuario, capacidades hardware, aplicaciones, etc.) puede diferir ligeramente en función de la personalización del sistema operativo realizada por el fabricante del terminal.
49. Antes de aplicar esta guía en un entorno de producción debe confirmarse su adecuación a la organización objetivo, siendo probada previamente en un entorno aislado y controlado donde se puedan realizar las pruebas necesarias y aplicar cambios en la configuración para que se ajusten a los criterios y requisitos específicos de cada organización.

[13] https://developers.google.com/android/nexus/images

Nota: el alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de los protocolos de comunicaciones basados en HTTPS (o SSL/TLS) y empleados por los dispositivos móviles Android, las aplicaciones móviles disponibles por defecto (o de terceros) y los diferentes servicios de Google (o de terceros).

5. CONFIGURACIÓN DE SEGURIDAD DE ANDROID

5.1 ACTUALIZACIÓN DEL SISTEMA OPERATIVO: ANDROID

50. Los dispositivos móviles Android, una vez disponen de conectividad de datos hacia Internet a través de las redes de telefonía móvil (2/3/4G) o de redes Wi-Fi, pueden verificar automáticamente si existe una nueva versión o actualización del sistema operativo.

51. Para ello, se establecen conexiones tanto cifradas mediante HTTPS (TCP/443), como no cifradas mediante HTTP (TCP/80), con el servidor "http[s]://android.clients.google.com".

52. Por ejemplo, una de las comprobaciones llevadas a cabo utiliza una petición al recurso "/checkin", de tipo POST, que permite obtener (entre otros) referencias horarias y emplea como parámetros datos en formato ProtoBuffer ("application/x-protobuffer"; comprimidos mediante GZIP[14]), es decir, el formato binario de intercambio de datos empleado por muchos servicios de Google y conocido como Google Protocol Buffers[15].

53. El agente de usuario (User-Agent) empleado para la comunicación HTTP en Android 4.4.4, dependiendo de la versión de la app Google Services Framework, GSF, y de la app Google Play services, es:

User-Agent: Android-Checkin/2.0 (hammerhead KTU84P); gzip
User-Agent: Dalvik/2.0.0 (Linux; U; Android 4.4.4; Nexus 5 Build/KTU84P)

NOTA: la referencia a "hammerhead" corresponde al nombre clave del dispositivo móvil Nexus 5, dispositivo móvil empleado para la elaboración de la presente guía.

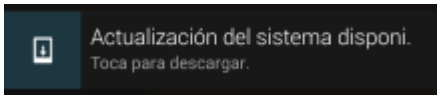
54. Esta opción es empleada frecuentemente para la distribución de actualizaciones de Android basada en mensajes OTA (Over-The-Air), y complementa la opción por parte del usuario de descargar manualmente el fichero correspondiente a la actualización completa directamente de los servidores oficiales de Google (analizada en detalle posteriormente).

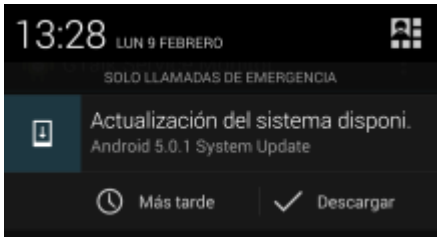
55. Es posible llevar a cabo esta operación de verificación de disponibilidad de actualizaciones en cualquier momento a través del menú "Ajustes - Información del teléfono - Actualizaciones del sistema":

[14] Dependiendo de la versión de las apps Google Services Framework y Google Play services.
[15] https://github.com/google/protobuf/

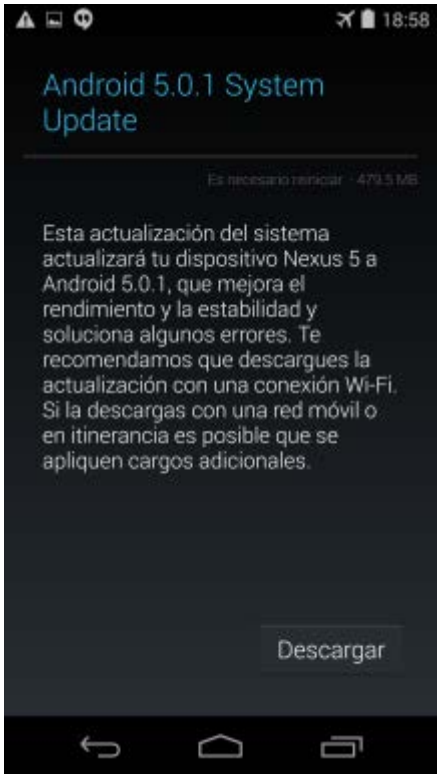
56. Mediante el código *#*#checkin#*#* (o *#*#2432546#*#*) del teclado del teléfono en Android es también posible forzar una búsqueda inmediata de actualizaciones y parches.

57. Si hay disponible una actualización, el dispositivo móvil mostrará en la barra superior de estado un mensaje notificando su disponibilidad, "Actualización del sistema disponible - Toca para descargar" o "Descargar":





58. Tras realizar la verificación, si existe una actualización disponible, el usuario puede llevar a cabo su descarga a través del botón "Descargar" de la pantalla de actualizaciones disponible desde el menú "Ajustes", o llegar a esta misma pantalla pulsando en la notificación correspondiente a la actualización:



59. Al pulsar el botón "Descargar", Android establece una conexión no cifrada HTTP con el servidor "http://android.clients.google.com" para descargar la misma, empleando el agente de usuario "AndroidDownloadManager/4.4.4" (desvelando la versión de Android y el modelo de dispositivo móvil; ver detalles en el ejemplo inferior), en este caso desde la versión de Android 4.4.4 (KTU84P) a la versión de Android 5.0.1 (LRX22C). Como respuesta se recibe una redirección (HTTP 302) a uno de los servidores de caché de Google para obtener la nueva actualización:

```
GET
/packages/ota/google_hammerhead/6dadaf477bab65f42f5681b03bd535f431594b95.
signed-hammerhead-LRX22C-from-KTU84P.6dadaf47.zip HTTP/1.1
Authorization: AJeBEBz-BfLRPlm8HtOy-aYMYhK96U9b2UFC-
I3YdOfh7KVwS4y0hpi38uiyOPTihKEJ_8z1jucDguZ_s75brxV83q7uOFT5GA
User-Agent: AndroidDownloadManager/4.4.4 (Linux; U; Android 4.4.4; Nexus
5 Build/KTU84P)
Accept-Encoding: identity
Host: android.clients.google.com
Connection: Keep-Alive
```

```
HTTP/1.1 302 Found
Location:
http://redirector.c.android.clients.google.com/packages/data/ota/google_h
ammerhead/6dadaf477bab65f42f5681b03bd535f431594b95.signed-hammerhead-
LRX22C-from-KTU84P.6dadaf47.zip
...
```

60. La petición hacia "redirector.c.android.clients.google.com" es a su vez redirigida a otro servidor de Google, por ejemplo "r17---sn-h5q7dn7z.c.android.clients.google.com", solicitando el mismo fichero ".zip", desde el mismo *path*, pero empleando una serie de parámetros GET en la petición:

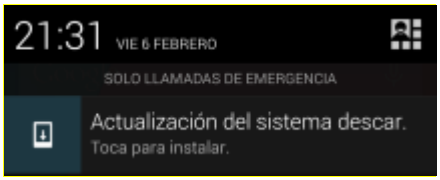
```
HTTP/1.1 302 Found
Location: http://r17---sn-
h5q7dn7z.c.android.clients.google.com/packages/data/ota/google_hammerhead
/6dadaf477bab65f42f5681b03bd535f431594b95.signed-hammerhead-LRX22C-from-
KTU84P.6dadaf47.zip?cms_redirect=yes&expire=1423162515&ip=<client-
IP>&ipbits=0&mm=31&ms=au&mt=1423148008&mv=m&nh=IgpwcjAxLm1hZDA2KgkxMjcuMC
4wLjE&pl=16&sparams=expire,ip,ipbits,mm,ms,mv,nh,pl&signature=6364C5F9C1E
3936206D3A734A6243E952ACBC65D.3968D0E5DED6503601B2A58CA73CA5CDA78B0EA2&ke
y=cms1
```

61. La integridad de las actualizaciones de las nuevas versiones de Android se verifica a través de una firma digital asociada al fichero de actualización (.zip) descargado, en concreto, mediante los certificados digitales (x.509) de sistema disponibles por defecto en "/system/etc/security/otacerts.zip"[16] (si no se especifica un conjunto de certificados distinto), que identifican quién puede distribuir y firmar actualizaciones OTA [Ref.- 45] [Ref.- 157].

62. La ausencia de cifrado puede permitir la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución del fichero asociado a la actualización OTA por otro fichero asociado a otra versión, también correspondiente a una actualización válida firmada digitalmente.

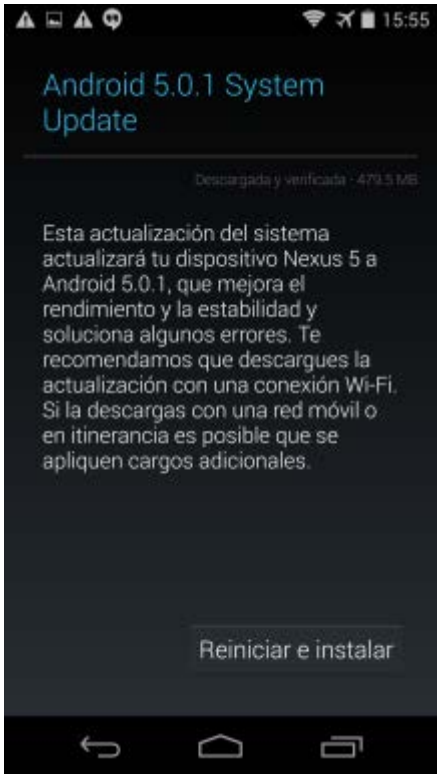
63. Por otro lado, la utilización de un canal no cifrado HTTP permite a un atacante conocer la versión y compilación actual (y potencialmente futura) del dispositivo móvil víctima, pudiendo explotar vulnerabilidades conocidas sobre dichas versiones.

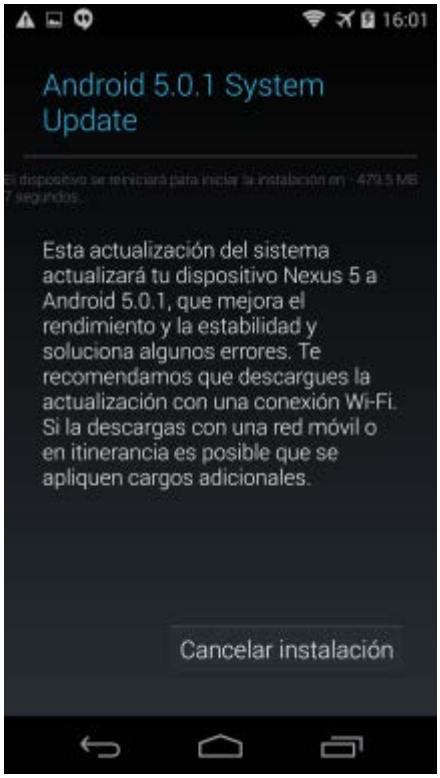
64. Una vez la actualización disponible ha sido descargada, se muestra una notificación en la barra superior de estado que indica que la actualización ha sido descargada y está disponible para su instalación ("Actualización del sistema descargada" - "Tocar para instalar")[17]:



[16] http://developer.android.com/reference/android/os/RecoverySystem.html

[17] En algunas versiones de Android y dispositivos móviles (ej. tabletas) la notificación puede incluir información sobre el número de la versión de Android asociada a la actualización y dos botones para proceder a su instalación ("Instalar"), o para posponer la misma ("Más tarde").





65. El fichero con la actualización OTA es almacenado en la partición "/cache" (partición únicamente accesible como root o superusuario), en concreto, en un fichero ".zip" cuyo nombre contiene el valor SHA1 del fichero ZIP de la actualización, junto al tipo de dispositivo móvil y referencias al número de compilación futuro y actual, respectivamente.

66. Ejemplo de actualización parcial (OTA) para Nexus 5 (hammerhead), desde la versión 4.4.3 (KTU84M) a la versión 4.4.4 (KTU84P) de Android (aunque los ejemplos previos mostraban la existencia de una actualización a Android 5.0.1 desde 4.4.4, debido a que el objetivo de la presente guía se centra en la versión 4.x de Android, no se emplearán referencias adicionales a Android 5, sino como en este caso, desde Android 4.4.3 a 4.4.4):

```
root@hammerhead:/cache # ls -l
ls -l
-rw------- u0_a8    u0_a8     2571501 2014-11-14 14:11
c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-hammerhead-KTU84P-from-
KTU84M.c08cce45.zip
```

67. Los detalles de este tipo de ficheros asociados a las actualización OTA son descritos posteriormente (ver apartado "5.1.3. Actualización manual parcial de Android").

68. Una vez el usuario confirma la instalación de la actualización a través del botón "Reiniciar e instalar" de la pantalla de actualizaciones, tras un margen de 10 segundos donde es aún posible cancelar la instalación, el dispositivo móvil se reiniciará, arrancará desde la partición de recuperación (o *recovery*) y procederá a llevar a cabo las tareas indicadas en el script disponible en el fichero de la actualización OTA [Ref.- 157].

69. Supuestamente, y en base a la documentación y referencias oficiales [Ref.- 69] (incluido el propio mensaje de anuncio inicial), las notificaciones y actualizaciones de seguridad de Android deberían estar disponibles en el grupo o lista de distribución "Android Security

Announcements", sin embargo, esta lista únicamente contiene una entrada sobre el anuncio inicial del equipo de seguridad de Android de agosto de 2008 [Ref.- 67].

70. Desafortunadamente no se dispone de un repositorio oficial de notificaciones con el listado de vulnerabilidades que han afectado a Android, y/o que han sido solucionadas, y en consecuencia, no existe un listado de actualizaciones disponibles para resolver esas vulnerabilidades.

71. Existe otro grupo o lista de distribución para la discusión de temas relacionados con seguridad en Android, denominado "Android Security Discussions" [Ref.- 68]. La problemática actual respecto al modelo de actualizaciones de seguridad de Android (reflejado posteriormente) ha sido analizada y discutida en numerosas ocasiones en dicho grupo.

72. Desde un punto de vista no oficial, existe un proyecto de la comunidad, denominado "Android Vulnerabilities" [Ref.- 65] que actúa como repositorio de las diferentes vulnerabilidades de seguridad que han afectado a las múltiples versiones de Android. El proyecto recibe contribuciones de la comunidad sobre nuevas vulnerabilidades, y permite clasificarlas por fabricante, año, versión de Android y contribuyente.

73. Oficialmente, las actualizaciones de Android, al tratarse de un sistema operativo de código abierto basado en Linux y con modificaciones particulares según los modelos de terminal, deben ser proporcionadas por los diferentes fabricantes de los dispositivos móviles [Ref.- 69] u operadores de telefonía móvil, en base a las modificaciones y ajustes realizados sobre las actualizaciones proporcionadas por el proyecto Android. Google, como líder del proyecto Android, no proporciona directamente actualizaciones para los dispositivos móviles Android (salvo para sus propios modelos de la familia Google Nexus).

Nota: debido a que el dispositivo móvil Android empleado para la elaboración de la presente guía es distribuido por Google directamente (actuando como fabricante del mismo, aunque en realidad sea fabricado por otra compañía con la que Google ha llegado a un acuerdo para cada modelo concreto), los procesos de actualización descritos en este documento afectan únicamente a los dispositivos móviles comercializados por Google, dentro de la familia Google Nexus [Ref.- 122], también conocidos como *Google Experience Devices* [Ref.- 71] o *Pure Android, 100% Google*. Los dispositivos Google Nexus están disponibles desde Google Play directamente (también referidos como *Google Play Devices* [Ref.- 70]).

Adicionalmente, existieron en el mercado dispositivos móviles conocidos como *Google Play* ***Edition*** *Devices*, es decir, comercializados por Google desde Google Play [Ref.- 70] pero creados por otros fabricantes, fuera de la familia Google Nexus. Estos dispositivos móviles también utilizan una versión no personalizada de Android, y por tanto, las actualizaciones para los mismos eran parejas en el tiempo a las proporcionadas por Google para la familia Google Nexus. Ejemplos de dispositivos móviles de este tipo han sido las ediciones especiales para Google Play del Samsung Galaxy S4, del HTC One o del Motorola Moto G, referenciados normalmente por su nombre seguidos del calificativo "edición Google Play". El programa de los *Google Play Edition Devices* parece haber finalizado en enero de 2015, con la retirada del último modelo disponible, el HTC One M8[18].

74. No existe ningún estándar ni modelo definido para la distribución de las actualizaciones de seguridad de Android, ni ninguna periodicidad definida para su publicación, por lo que

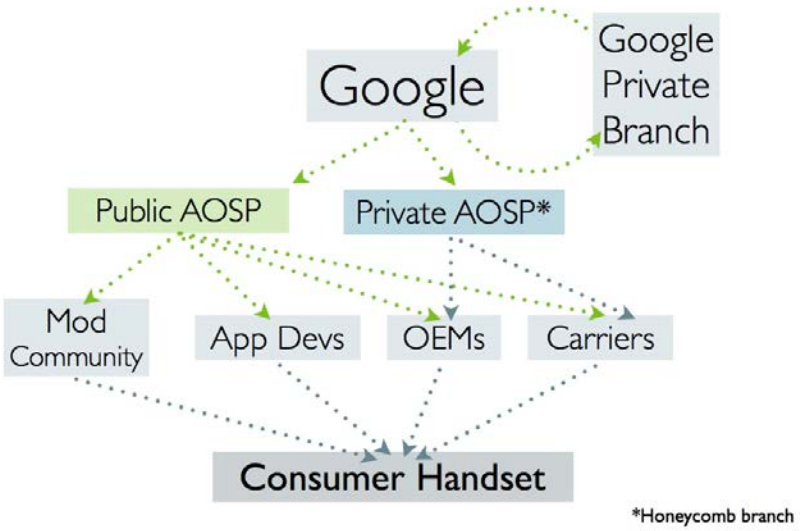
[18] https://play.google.com/store/devices/details?id=htc_m8 (enlace todavía activo a fecha 30/01/2015).

Google y otros fabricantes (miembros o no de la *Open Handset Alliance*) pueden seguir procedimientos de actualización diferentes.

75. Pese a que en varias ocasiones, e incluso públicamente, los fabricantes de dispositivos móviles de la *Open Handset Alliance* han intentado llegar a un acuerdo y comprometerse a proporcionar actualizaciones durante al menos 18 meses (periodo mínimo de soporte) desde la comercialización inicial de cada modelo de terminal, el tiempo y la historia han confirmado que no han sido capaces de mantener y ratificar ni siquiera estos compromisos.

76. El fabricante del dispositivo móvil o el operador de telefonía es el que publicará actualizaciones para el terminal. Como norma general, y salvo que exista un motivo que desaconseje su instalación, se recomienda aplicar sobre el dispositivo móvil todas las actualizaciones facilitadas por el fabricante, ya que pese a que las mismas no reflejen explícitamente que se trata de actualizaciones de seguridad, pueden solucionar vulnerabilidades de seguridad públicamente conocidas.

77. Google ha desarrollado un modelo para la resolución de problemas de seguridad y la distribución de actualizaciones en Android a través de CTS (Compatibility Test Suite) [Ref.- 86], actividad integrada en el Android Open Source Project (AOSP), encargada de asegurar la compatibilidad entre dispositivos Android [Ref.- 85]:



78. Sin embargo, toda la complejidad asociada a las actualizaciones de Android y los diferentes factores y entidades involucradas en el proceso, como las múltiples personalizaciones del sistema operativo realizadas por los fabricantes, dan lugar a retrasos significativos desde que las soluciones de seguridad son añadidas al repositorio del *Android Open Source Project* (AOSP[19]) hasta que están disponibles para los usuarios, dejando los dispositivos móviles desprotegidos durante todo ese tiempo (varios meses en el mejor de los casos).

79. La siguiente imagen refleja las vulnerabilidades más significativas en Android durante el periodo entre los años 2010 y 2011, algunas de las cuales han sido aprovechadas por código dañino públicamente distribuido, como DroidKungFu y DroidDream [Ref.- 85]:

[19] https://source.android.com

Known Android Vulnerabilities 2010-2011		
Year	Vulnerability	Malware that Exploited Vuln
2010	Exploid	DroidDream, zHash, DroidKungFu (Legacy)
2010	CVE-2010-1807 WebKit NaN	
2010	RageAgainstTheCage/Zimperlich	DroidDream, BaseBridge, DroidKungFu (Legacy)
2011	Psneuter/KillingInTheNameOf	
2011	Gingerbreak/Honeybomb	

80. Mediante la realización de una búsqueda por el término "Android" en la US CERT NVD (National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search-results?query=android&search_type=all&cves=on) o en el proyecto CVE (*Common Vulnerabilities and Exposures*) de MITRE (http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android) es posible obtener un listado de las vulnerabilidades de seguridad conocidas públicamente que han afectado a diferentes versiones del sistema operativo Android en los últimos años, así como a aplicaciones de terceros desarrolladas para Android.

81. Adicionalmente, las soluciones publicadas para corregir vulnerabilidades de seguridad conocidas suelen estar disponibles únicamente para las últimas versiones de Android, no existiendo un mecanismo establecido para proporcionar dichas soluciones para versiones previas de Android, también vulnerables.

82. Por otro lado, numerosos fabricantes y operadores de telefonía móvil no proporcionan actualizaciones para modelos de dispositivos móviles previos, por ejemplo, basados en las versiones 2.x de Android, por lo que estos serán siempre vulnerables.

83. Este hecho se ve agravado por la velocidad de consumo de las nuevas tecnologías, que afecta a cuando los dispositivos móviles son considerados obsoletos, dónde en la actualidad, un dispositivo con dos o más años difícilmente estará soportado e incluido en el ciclo de actualizaciones de software.

84. Por ejemplo, en octubre de 2011 Google confirmó que el dispositivo móvil empleado para la elaboración de la versión previa de la presente guía, Google (HTC) Nexus One (lanzado al mercado por Google en enero de 2010), no dispondría de una actualización oficial a Android 4.0 ("Ice Cream Sandwich") [Ref.- 100]. Ésta versión de Android sí estaría disponible para otros modelos, como el Nexus S y el Galaxy Nexus.

85. Posteriormente, en un caso similar, en septiembre de 2013 Google confirmó que el dispositivo móvil Google Galaxy Nexus (lanzado al mercado por Google en noviembre de 2011 como el primer dispositivo móvil con Android 4.0), no dispondría de una actualización oficial a Android 4.4 ("KitKat"), originando protestas colectivas por parte de la comunidad [Ref.- 95]. Google argumentó que el Galaxy Nexus había superado el periodo de soporte de 18 meses desde su comercialización. Ésta versión de Android sí estaría disponible para otros modelos, como el Nexus 4 y el Nexus 7.

86. La importancia, por un lado, de actualizar la versión de Android en el dispositivo móvil a la última versión disponible, y por otro, de verificar si la actualización corrige vulnerabilidades previas públicamente conocidas, se refleja tanto en vulnerabilidades

antiguas relevantes y muy generalizadas como la de TapJacking [Ref.- 113], como en vulnerabilidades críticas más recientes que han afectado a Android, como por ejemplo "Android Master Key" [Ref.- 114], "Android browser SOP bypass" (o Universal XSS, UXSS, en Android < 4.4) [Ref.- 115] (CVE-2014-6041) o sus variantes [Ref.- 97], vulnerabilidades en Android WebView (en Android < 4.4) [Ref.- 116], "Android Fake ID" [Ref.- 98], y otras vulnerabilidades y exploits publicados para Android durante el año 2014 [Ref.- 62].

87. En el caso de disponer de un dispositivo móvil Android para el que se sí dispone de una actualización a una versión superior de Android, por ejemplo 4.4.4 para un terminal basado en Android 4.3, se recomienda aplicar la actualización sobre el dispositivo con el objetivo de instalar la última versión disponible y protegerlo de vulnerabilidades conocidas.

88. En el caso de los dispositivos móviles Google Nexus, las diferentes versiones del sistema operativo Android pueden ser proporcionadas mediante una imagen completa del sistema operativo (o plataforma móvil) Android (ver apartado "5.1.2. Actualización manual completa de Android"), o como una imagen parcial, normalmente obtenida como actualización OTA (*Over The Air*) (ver apartado "5.1.3. Actualización manual parcial de Android").

89. Si la imagen es parcial, todos los datos y configuración del usuario son conservados, mientras que si la imagen es completa, se eliminarán todos los datos y configuración del usuario, fijando los valores de configuración de fábrica durante el proceso. Una imagen completa instala una nueva versión de Android en el dispositivo móvil como si se tratase de un dispositivo recién comprado u obtenido de fábrica.

90. Debe tenerse en cuenta que antes de realizar una actualización del sistema operativo del dispositivo móvil se recomienda realizar una copia de seguridad de los datos del usuario.

91. Pese a que existen foros en Internet dónde se distribuyen imágenes de ROM o *firmware* para múltiples sistemas operativos y fabricantes de terminales (como XDA Developers - http://forum.xda-developers.com), desde el punto de vista empresarial, en ningún caso se recomienda la instalación del sistema operativo desde una fuente no oficial.

92. En el mundo Android, las actualizaciones individuales adicionales a las actualizaciones de la versión completa del sistema operativo son muy limitadas, en contraposición a las actualizaciones para otros sistemas operativos de sobremesa cliente o servidor. Esta situación afecta tanto a las actualizaciones generales sobre los distintos componentes del sistema operativo, como a las actualizaciones específicas de seguridad.

93. Con el objetivo de mantener el dispositivo móvil actualizado, se recomienda comprobar periódicamente desde el propio dispositivo la disponibilidad de actualizaciones desde el menú "Ajustes - Información del teléfono - Actualizaciones del sistema".

94. Desde el punto de vista de seguridad es necesario actualizar igualmente todas las aplicaciones móviles (o apps) instaladas sobre el sistema operativo (ver apartado "5.22.5. Actualización de apps en Android") y, en particular, la app asociada a los servicios de Google Play debido a las capacidades de actualización de que dispone en la propia plataforma móvil Android (descritas a continuación).

5.1.1 SERVICIOS DE GOOGLE PLAY

95. En los últimos años Google ha adoptado un modelo de actualizaciones diferente y desconocido en muchas ocasiones. A través de la app Google Play, y de sus servicios asociados, la plataforma móvil Android recibe numerosas actualizaciones que no sólo

afectan a Google Play y al mercado de apps, sino también a otros componentes (o apps) críticas del sistema operativo y existentes por defecto [Ref.- 60].

96. Por tanto, el concepto de actualización en Android ha cambiado. Muchos componentes de la arquitectura de Android se han independizado del núcleo de la plataforma móvil, pudiendo ser actualizados independientemente y con mayor frecuencia. En lugar de tener que actualizar el sistema operativo a una nueva versión para poder disponer de funcionalidades o mecanismos de seguridad previamente ausentes, la actualización individual de la app de Google Play (denominada "Play Store") puede proporcionar nuevas actualizaciones para ciertos elementos de la plataforma móvil.

97. Por ejemplo, los teclados del sistema, el navegador web (Chrome), la app de correo electrónico (Gmail) y de mensajería (Hangouts), la app de calendario, e incluso la app de los ajustes de configuración (Google Settings, "Ajustes de Google"), pueden ser actualizadas independientemente como cualquier otra app de terceros.

98. Este tipo de actualizaciones parciales a través de la app de Google Play ("Play Store", y de los servicios de Google Play, *Google Play Services*[20] [Ref.- 148]) son distribuidas incluso para dispositivos móviles que disponen de versiones antiguas de Android (desde Android 2.3 - Gingerbread) y para las que no se dispone de nuevas actualizaciones de sistema operativo, por ejemplo a Android 4.x.

99. A lo largo del presente informe se describen algunas capacidades y ajustes de configuración existentes en Android que han sido actualizados a través de esta vía, como por ejemplo el administrador de dispositivo Android (existente por defecto en Android 4.4) o las capacidades de escaneo o verificación de apps (ver apartado "5.23.4. Verificación de seguridad de las apps").

100. Otra de las vulnerabilidades que fue resuelta a través de las capacidades de actualización de los servicios de Google Play es la asociada (originalmente) a la versión 4.4.4 de Android, y específicamente a la vulnerabilidad de OpenSSL que permitía la realización de ataques MitM (Man-in-the-Middle), con CVE-2014-0224 y conocida como la vulnerabilidad de "inyección CCS (ChangeCipherSpec)" [Ref.- 136] [Ref.- 137].

101. El proveedor de seguridad que proporciona las capacidades de comunicaciones de red seguras de Android fue actualizado con la versión 5.0 de los servicios de Google Play (publicada en julio de 2014[21]) para mitigar específicamente esta vulnerabilidad de inyección CSS" [Ref.- 150].

102. Se recomienda que las apps hagan uso de los métodos asociados a los servicios de Google Play, por un lado, para confirmar que se dispone de la última versión del proveedor de seguridad, y por otro, para asegurarse de que ejecutan en un dispositivo móvil que hace uso de dicho proveedor de seguridad, actualizado, y que mitiga ataques basados en vulnerabilidades y *exploits* conocidos.

5.1.2 ACTUALIZACIÓN MANUAL COMPLETA DE ANDROID

103. Alternativamente a la actualización automática realizada por Android (o cuando ésta no está disponible para ciertos fabricantes u operadores de telefonía móvil), es posible realizar la actualización del sistema operativo de Android de forma manual mediante la descarga

[20] https://play.google.com/store/apps/details?id=com.google.android.gms&hl=es
[21] https://developer.android.com/google/play-services/index.html

de los ficheros de actualización oficiales desde la web de Google [Ref.- 72] (o del fabricante).

104. En el caso de ciertos fabricantes u operadores de telefonía móvil, en la mayoría de ocasiones estos ficheros no son publicados oficialmente, aunque su ubicación puede estar disponible de manera no oficial desde numerosas fuentes en Internet.

105. Para versiones previas de Android, como por ejemplo 2.x, existía una lista no oficial (incompleta) con los ficheros de actualización proporcionados por Google y los diferentes fabricantes de dispositivos móviles basados en Android (ver versión previa de la presente guía para Android 2.x).

106. Desde el punto de vista de seguridad, las descargas de actualizaciones siempre deben realizarse desde enlaces que referencien a la web oficial de Google (o del fabricante), y es recomendable actualizar siempre a la última versión disponible.

107. En el caso de los dispositivos móviles comercializados por Google, desde hace unos años Google proporciona de manera oficial acceso a las imágenes completas de fábrica para las actualizaciones y nuevas versiones de Android, en concreto, para los dispositivos móviles de la familia Google Nexus, *Factory Images for Nexus Devices* [Ref.- 72].

108. La página web con las imágenes completas de fábrica para los dispositivos móviles Google Nexus se va actualizando periódicamente según se van publicando nuevas versiones de Android, pudiendo desaparecer las referencias e imágenes de versiones o subversiones previas.

109. Debe tenerse en cuenta que el proceso de actualización del dispositivo móvil a partir de una imagen de *firmware* completa eliminará todos los datos del terminal, por lo que se recomienda realizar una copia de seguridad antes de llevar a cabo este proceso.

110. En el caso de los dispositivos móviles Google Nexus, las diferentes versiones del sistema operativo Android pueden ser proporcionadas mediante una imagen completa del sistema operativo (o plataforma móvil) Android, o como una imagen parcial, normalmente obtenida como actualización OTA (*Over The Air*) (ver apartado "5.1.3. Actualización manual parcial de Android").

111. Si la imagen es completa, se dispone de los enlaces a las imágenes oficiales directamente desde Google [Ref.- 72] para los distintos modelos de dispositivo móvil, descargables desde "https://dl.google.com/dl/android/aosp/*", como por ejemplo la versión Android 4.4.4 (KTU84P) empleada para la elaboración de la presente guía en un terminal Nexus 5:

https://dl.google.com/dl/android/aosp/hammerhead-ktu84p-factory-35ea0277.tgz

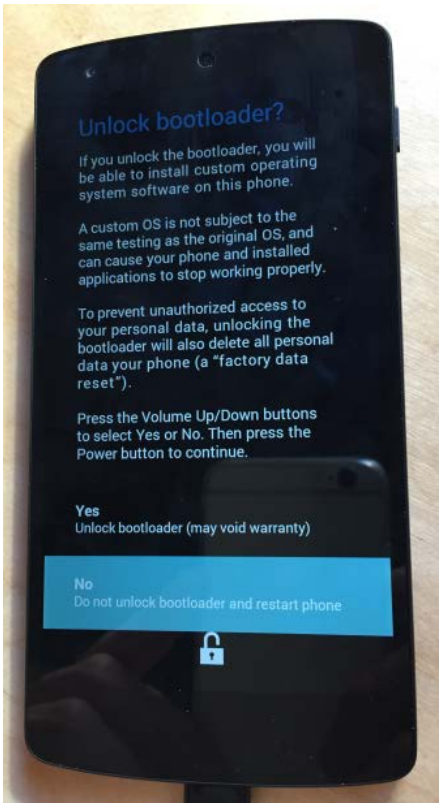
112. El nombre del fichero corresponde al nombre clave del tipo de dispositivo móvil, en este caso "hammerhead" asociado al Nexus 5, seguido del número de compilación "KTU84P" (Android 4.4.4), el indicativo de que se trata de la imagen completa o de fábrica ("factory"), y por último, los 8 primeros caracteres del hash SHA1 de dicho fichero ".tgz" (35ea0277bd6a8fc928b47256bfa97b2eed60746b).

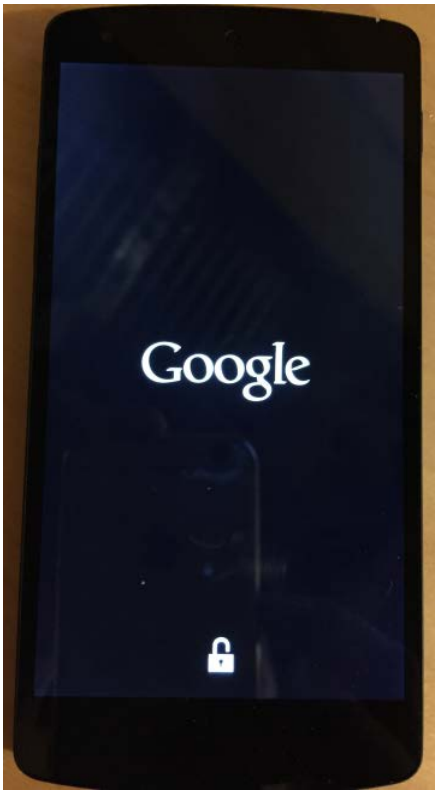
113. Para llevar a cabo el proceso de actualización (desde Windows, Linux o OS X) es necesario disponer de la herramienta fastboot, contenida en el SDK (*Software Development Kit*) de Android y empleada por el script "flash-all", y habilitar el acceso USB al dispositivo móvil como desarrollador [Ref.- 72].

114. Una vez el dispositivo móvil se ha conectado mediante el puerto USB, es necesario reiniciarlo desde la imagen o gestor de arranque (o *bootloader*), también conocido como modo fastboot (para dispositivos móviles Nexus), ya sea mediante el comando "adb reboot bootloader"[22], o desde el propio dispositivo móvil[23], apagando el terminal y encendiéndolo (en el caso del dispositivo móvil empleado para la elaboración de la presente guía) manteniendo pulsados los botones de bajar y subir el volumen simultáneamente, y posteriormente manteniendo pulsado el botón de encendido.

115. Este proceso de actualización requiere desbloquear el gestor de arranque (o *bootloader*) del dispositivo móvil, si aún no ha sido desbloqueado previamente. Pera ello es necesario confirmar que el dispositivo móvil está disponible en modo fastboot mediante el comando "fastboot devices", y ejecutar el comando "fastboot oem unlock". Tras recibir la confirmación del usuario a través de la pantalla del terminal (ver imagen inferior izquierda), se eliminarán todos los datos existentes en el dispositivo móvil y se desbloqueará el *bootloader*.

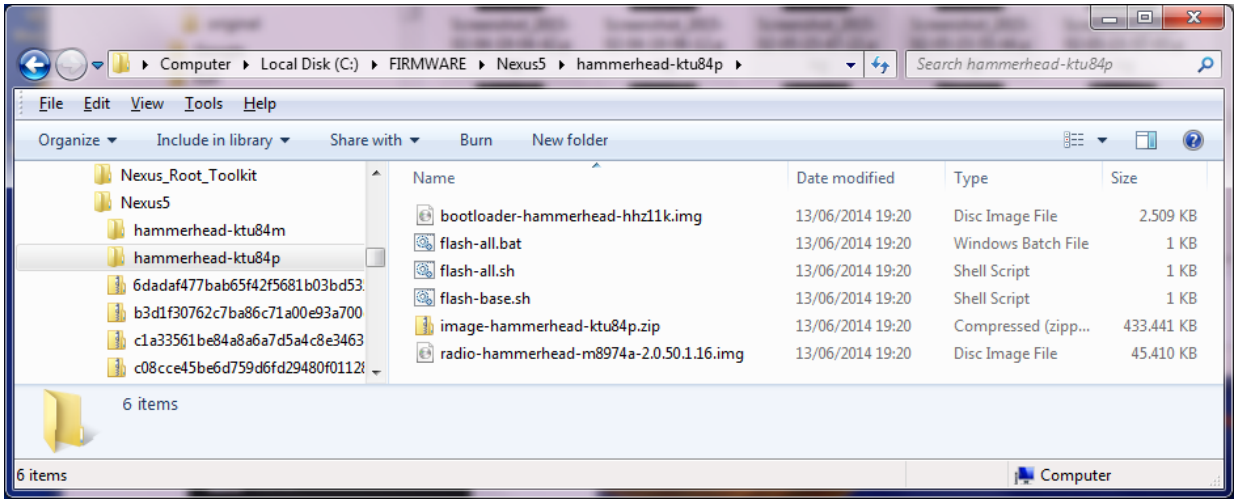
116. Cuando el *bootloader* está desbloqueado es indicado mediante un candado abierto, frente a un candado cerrado (o inexistente), en la parte inferior central del dispositivo móvil, durante el proceso de arranque:





117. Una vez descargada la imagen completa del *firmware* de la versión de Android a instalar, debe descomprimirse el fichero ".tgz", y acceder al directorio asociado recién creado:

[22] En algunos dispositivos móviles Android el comando "adb reboot fastboot" puede ser equivalente, pero no en el caso del dispositivo móvil empleado para la elaboración de la presente guía.
[23] https://source.android.com/source/building-devices.html#booting-into-fastboot-mode



118. Mediante la ejecución del script "flash-all" (.bat o .sh) se llevará a cabo la instalación del gestor de arranque (*bootloader*), del *firmware* del procesador de banda base (*baseband*) o radio, y del sistema operativo Android.

119. El apartado "8. Apéndice C: Actualización manual completa a Android 4.4.4" contiene a modo de ejemplo la salida completa de la ejecución del script "flash-all" al actualizar el dispositivo móvil Android a la versión 4.4.4.

Nota: el proceso de actualización desde una imagen completa de Android mediante el script "flash-all" también elimina todos los datos de usuario del terminal por defecto. Esta es la opción de actualización recomendada con el objetivo de evitar problemas de compatibilidad entre diferentes versiones de Android debido a la existencia de contenidos y datos previamente existentes. Sin embargo, existe la posibilidad de modificar el script "flash-all" y en concreto la directiva "fastboot -w update ...", eliminado la opción "-w" (*wipe*), para que los datos de usuario no sean borrados durante el proceso de actualización.

120. Una vez el dispositivo móvil ha sido actualizado, se reiniciará y ejecutará la nueva versión de Android. El dispositivo móvil arrancará en su estado original de fábrica, por lo que será necesario completar el proceso de configuración inicial (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial").

121. Desde el punto de vista de seguridad se recomienda bloquear de nuevo el gestor de arranque (*bootloader*) nada más completar el proceso de actualización, arrancando de nuevo el dispositivo móvil en modo fastboot, y ejecutando el comando "fastboot oem lock". Este proceso no eliminará ningún dato del terminal.

122. Para proceder a bloquear de nuevo el gestor de arranque (o *bootloader*) no es necesario completar el proceso de instalación y configuración inicial. Basta con apagar el dispositivo móvil tras el primer reinicio después de la actualización, arrancar de nuevo en modo fastboot desde el propio dispositivo móvil con la combinación de botones descrita previamente, y conectar el dispositivo móvil a un ordenador mediante el puerto USB. Desde el mismo, es posible ejecutar el comando "fastboot oem lock" para volver a bloquear inmediatamente el gestor de arranque. El estado es indicado en el propio gestor de arranque (“LOCK STATE”):

123. De esta forma, una vez el *bootloader* está bloqueado, no es posible actualizar el dispositivo móvil mediante una actualización completa, ni interactuar con las diferentes particiones existentes en el terminal, sin tener que eliminar previamente todos los datos del usuario.

5.1.3 ACTUALIZACIÓN MANUAL PARCIAL DE ANDROID

124. Alternativamente a la actualización automática realizada directamente por Android, o al proceso de actualización manual desde una imagen completa de *firmware* detallado en el apartado previo, es posible realizar la actualización del sistema operativo de Android de forma manual mediante la descarga de los ficheros de actualización OTA (*Over The Air*) parciales oficiales desde la web de Google (o del fabricante), obtenidos mediante el análisis del tráfico de red del proceso de actualización OTA.

125. En el caso de los dispositivos móviles Google Nexus, las diferentes versiones del sistema operativo Android pueden ser proporcionadas mediante una imagen completa del sistema operativo (o plataforma móvil) Android (ver apartado "5.1.2. Actualización manual completa de Android"), o como una imagen parcial, normalmente obtenida como actualización OTA.

126. Si la imagen es parcial, contiene únicamente las actualizaciones incrementales a aplicar en el *firmware* (o versión del sistema operativo) actual del dispositivo móvil, y debe ser cargada en el terminal actualizando la versión de Android existente actualmente.

127. El tamaño de las actualizaciones parciales es muy inferior al de las actualizaciones completas, y se dispone de diferentes actualizaciones parciales para una misma versión final y objetivo de Android, en función de la versión de Android actual disponible en el dispositivo móvil, y del modelo de dispositivo móvil.

128. Por ejemplo, para el dispositivo móvil empleado para la elaboración de la presente guía, existe una imagen de actualización parcial a Android 4.4.2 (KOT49H) desde Android 4.4.1 (KOT49E), y otra diferente desde Android 4.4 (KRT16M) [24].

129. Habitualmente, estas imágenes parciales son distribuidas a través de OTA, y no se dispone de los enlaces a las imágenes parciales oficiales directamente desde Google para los distintos modelos de dispositivo móvil (tal como sí ocurre con las imágenes completas).

130. Sin embargo, por un lado, existen repositorios no oficiales con referencias, en concreto para los dispositivos móviles de la familia Google Nexus (de interés y aplicación en la presente guía) o Google Experience Devices, que permiten identificar las diferentes imágenes parciales disponibles [Ref.- 120], al igual que obtener las referencias a los enlaces OTA oficiales de Google, desde foros como XDA Developers [Ref.- 184].

131. Por otro lado, mediante el análisis de los registros o logs de logcat, o del tráfico de red del proceso de actualización de Android, es posible obtener los enlaces a los ficheros de descarga de las actualizaciones OTA, que están disponibles desde el servidor "http://android.clients.google.com/packages/ota/*", como por ejemplo la actualización a la versión Android 4.4.4 (KTU84P) desde la versión Android 4.4.3 (KTU84M), empleada para la elaboración de la presente guía en un Nexus 5 (hammerhead):

> http://android.clients.google.com/packages/ota/google_hammerhead/c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-hammerhead-KTU84P-from-KTU84M.c08cce45.zip

132. El nombre del directorio incluye el término "google_", seguido del nombre clave del tipo de dispositivo móvil, en este caso "hammerhead" asociado al Nexus 5. El nombre del fichero corresponde al valor SHA1 (c08cce45be6d759d6fd29480f01128b18f7d4a11) del propio fichero ZIP de la actualización, una indicación de que ha sido firmado (".signed"), de nuevo el nombre clave del tipo de dispositivo ("hammerhead"), seguido del número de compilación "KTU84P" (Android 4.4.4) futuro y actual, "KTU84M" (Android 4.4.3), respectivamente. Por último, el nombre del fichero también incluye al final los 8 primeros caracteres del hash SHA1 de dicho fichero ".zip".

133. El proceso de actualización parcial (desde Windows, Linux o OS X) requiere disponer del fichero de actualización parcial oficial descargado desde la web de Google, y es también necesario disponer del SDK de Android y habilitar todo el entorno utilizado para el acceso por USB al dispositivo móvil como desarrollador, en concreto, mediante ADB.

134. Una vez el dispositivo móvil se ha conectado mediante el puerto USB, es necesario reiniciarlo desde la imagen de recuperación (o *recovery*).

135. La imagen de recuperación (o *recovery*) es accesible directamente, o desde gestor de arranque (o *bootloader*), también conocido como modo fastboot (para dispositivos móviles Nexus).

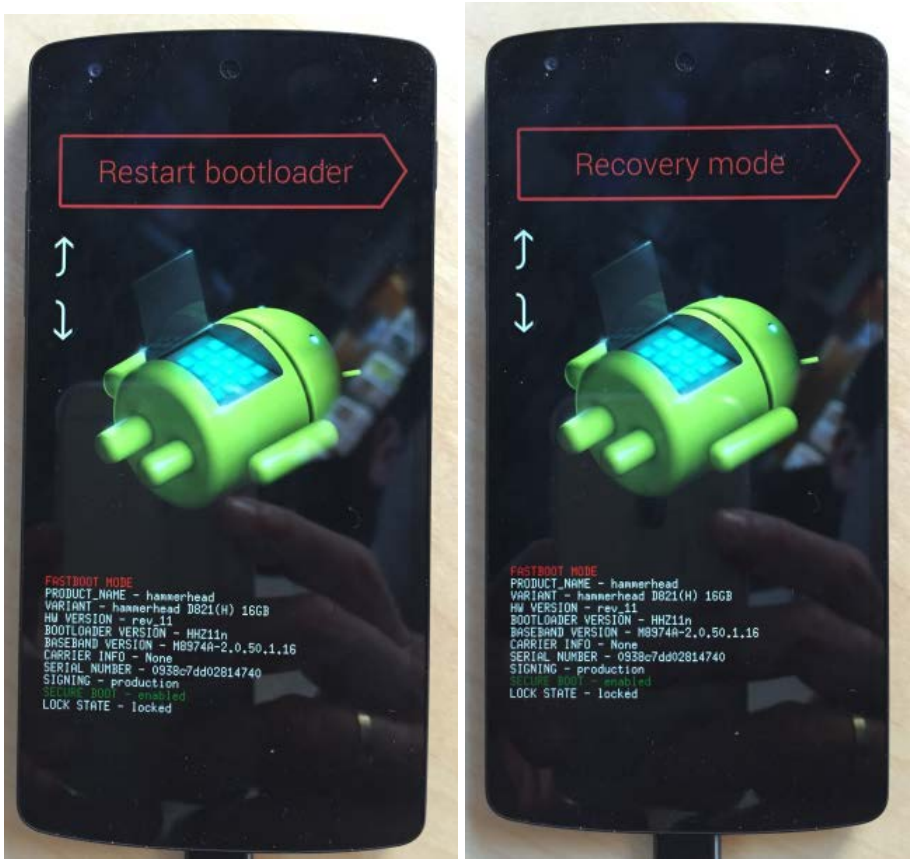
136. En el caso de acceder directamente, es necesario disponer de acceso mediante USB y ADB, y emplear el comando "adb reboot recovery", accediéndose directamente a la pantalla de la imagen de recuperación con un androide y un icono de peligro (descrita posteriormente).

[24] http://www.randomphantasmagoria.com/firmware/nexus-5/hammerhead/

137. En el caso de acceder a través del *bootloader*, puede emplearse el comando "adb reboot bootloader" (como se describió en el apartado previo), o desde el propio dispositivo móvil[25], apagando el terminal y encendiéndolo (en el caso del dispositivo móvil empleado para la elaboración de la presente guía) manteniendo pulsados los botones de bajar y subir el volumen simultáneamente, y posteriormente manteniendo pulsado el botón de encendido.

138. Una vez en el *bootloader*, debe accederse a la imagen de recuperación (*recovery image*), también conocida como modo recuperación o consola de recuperación. Para ello se deben emplear los botones de volumen para cambiar entre las diferentes opciones, y el botón de encendido para seleccionar la opción "Recovery mode":

[25] https://source.android.com/source/building-devices.html#booting-into-fastboot-mode



139. El dispositivo móvil se reiniciará y mostrará una pantalla de recuperación que muestra un androide y un icono de peligro, con una admiración dentro de un triángulo (/!\) de color rojo. A continuación debe mantenerse pulsado el botón de encendido y posteriormente pulsar el botón de subir el volumen simultáneamente.

140. Una vez aparece el menú de la imagen de recuperación, en color rojo y azul, con el texto "Android system recovery <3e>" y el número de compilación de la versión de Android empleada, debe seleccionarse la opción "apply update from ADB", de nuevo mediante los botones de volumen, para cambiar entre las diferentes opciones, y usando el botón de encendido para seleccionar la opción deseada.

141. Cuando el dispositivo se encuentra en la imagen de recuperación, y se habilitan las capacidades de comunicación mediante ADB, el estado del dispositivo es diferente al empleado en el acceso ADB estándar, y viene identificado por el término "sideload".

142. Para llevar a cabo una actualización manual parcial en el dispositivo móvil, tal como ocurre con las actualizaciones OTA, no es necesario desbloquear el gestor de arranque (o *bootloader*).

143. A continuación es necesario ejecutar desde el ordenador el comando que lleva a cabo la carga de la actualización parcial a través del puerto USB: "adb sideload <nombre_de_fichero>.zip", donde "<nombre_de_fichero>.zip" corresponde al nombre del fichero ZIP con la actualización parcial a aplicar. Este comando debe ejecutarse directamente desde el directorio dónde se descargó dicho fichero:

```
C:\FIRMWARE\Nexus5>adb devices
List of devices attached
0938c7dd02814740        sideload
```

```
C:\FIRMWARE\Nexus5>adb sideload
c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-
hammerhead-KTU84P-from-KTU84M.c08cce45.zip
...
loading: 'c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-hammerhead-
KTU84P-from-KTU84M.c08cce45.zip'
sending: 'c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-hammerhead-
KTU84P-from-...
...
sending: 'c08cce45be6d759d6fd29480f01128b18f7d4a11.signed-hammerhead-
KTU84P-from-KTU84M.c08cce45.zip'  100%

C:\FIRMWARE\Nexus5>
```

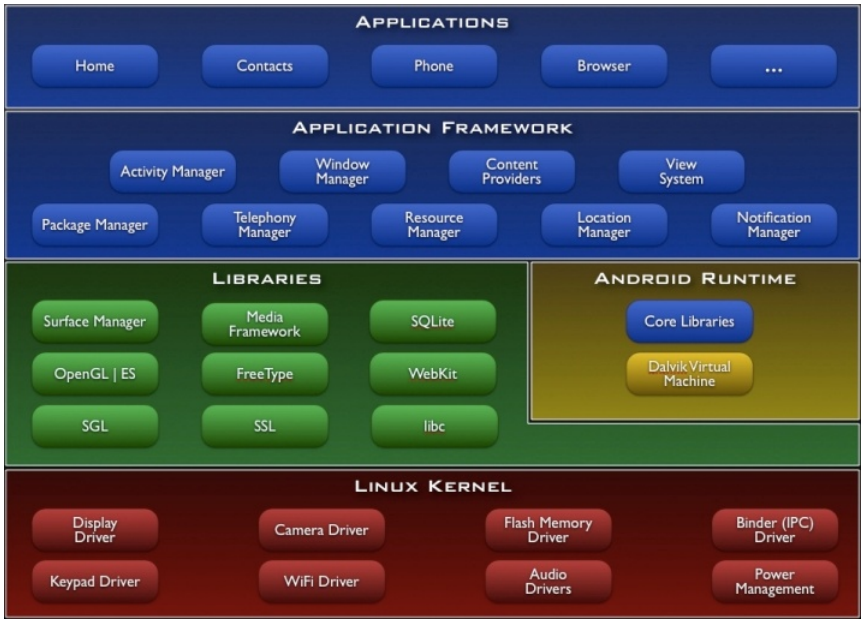
Nota: en algunos casos (dependiendo de las modificaciones realizadas por la actualización y de la versión exacta previa y final de Android) puede ser recomendable adicionalmente, una vez se ha completado la misma, y desde la imagen de recuperación, limpiar la caché del dispositivo móvil a través de la opción "wipe cache partition".

144. Una vez se ha completado la instalación de la actualización, estado identificado por el mensaje "Install from ADB complete.", se debe seleccionar la opción "reboot system now" para reiniciar el dispositivo móvil con la nueva actualización aplicada, proceso que puede llevar algún tiempo.

145. Cuando el dispositivo móvil ha sido actualizado, tras reiniciarlo, éste ejecutará la nueva versión de Android, conservando los datos de usuario existentes previamente, tal como ocurriría con una actualización parcial recibida mediante OTA.

5.2 MODELO Y ARQUITECTURA DE SEGURIDAD DE ANDROID

146. El modelo o arquitectura de seguridad de Android está basado en el sistema operativo Linux [Ref.- 17] y proporciona adicionalmente numerosas librerías y entornos de ejecución para las aplicaciones móviles [Ref.- 11]:



147. Android aplica el principio de mínimo privilegio por defecto, donde cada aplicación móvil (o app) únicamente dispone de acceso a sus propios componentes, incrementando así la

seguridad general de la plataforma, y limitando las acciones que una app puede realizar sobre otras apps, en el sistema o en su interacción con el usuario.

5.2.1 MODELO DE PERMISOS DE ANDROID

148. La seguridad más granular de la plataforma se basa en un mecanismo de permisos que impone restricciones en las operaciones que un proceso (o app) puede llevar a cabo, incluyendo también restricciones en el acceso a datos (en función de su identificador o URI, *Uniform Resource Identifier*) para los proveedores de contenidos (descritos posteriormente).

149. Las apps por tanto deben definir y solicitar permiso para acceder a los recursos y datos compartidos en los que están interesadas. El sistema notifica al usuario estos permisos en el momento de la instalación de la app. Una vez el usuario autoriza a una app a disponer de dichos permisos, ésta será instalada y podrá hacer uso de los mismos en cualquier momento durante su ejecución (presente y futuras). En ningún caso se solicitará autorización al usuario durante la ejecución de la app, sino únicamente en el momento de su instalación.

150. Android no proporciona granularidad suficiente para seleccionar únicamente un subconjunto de todos los permisos solicitados por una app y restringir así su funcionalidad (ver apartado "5.2.6. App Ops"). Si se instala una app, ésta dispondrá de acceso a todos los permisos solicitados. Si el usuario no está interesado en proporcionar ciertos permisos a una app, la única opción disponible es no instalar dicha app.

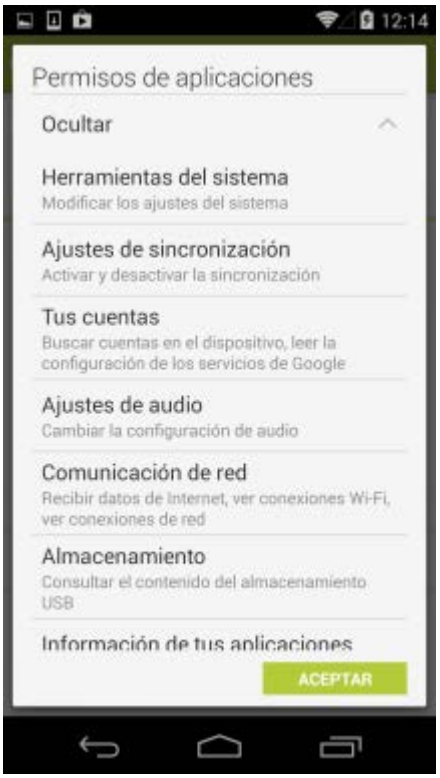
151. Adicionalmente, para ciertos permisos, como el de acceso a Internet, sería deseable disponer de suficiente granularidad en Android para poder autorizar a una app a conectarse a Internet sólo a ciertos sitios web, y no a cualquier destino. Esta funcionalidad no está disponible en el modelo de permisos actual de Android.

152. La única excepción al modelo de permisos general descrito es la asociada a ciertos permisos disponibles para los desarrolladores (como por ejemplo "READ_LOGS", "WRITE_SECURE_SETTINGS", etc), introducidos en Android 4.2, y que si pueden ser habilitados o deshabilitados bajo demanda en cualquier momento y de manera dinámica, mediante el comando "pm grant/revoke", *Package Manager* [Ref.- 26].

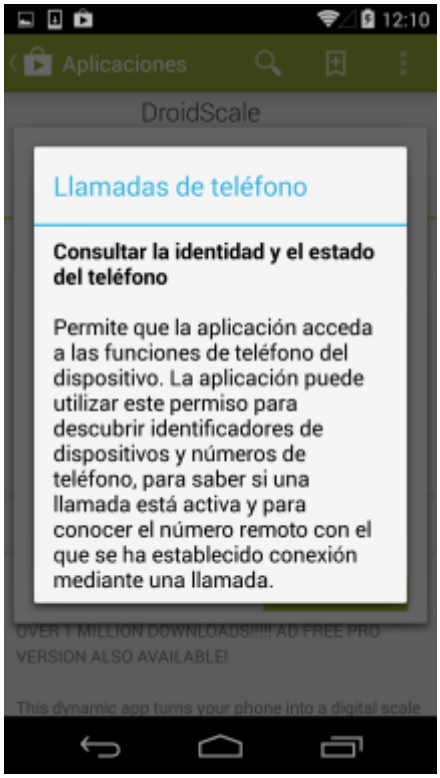
153. El siguiente ejemplo[26] muestra los diferentes permisos solicitados por una app Android concreta durante el proceso de instalación. En la aplicación móvil para la descarga de apps de Android, "Play Store", tras pulsar el botón de instalación en la página de descripción de la app, se solicita la aceptación por parte del usuario de los permisos demandados por la app (ejemplo empleando la app "Play Store" versión 4.5.10[27]):

[26] Se ha empleado la app falsa "DroidScale" que supuestamente convierte el dispositivo móvil en una báscula para pesar objetos (funcionalidad inexistente), y que ha sido descargada más de un millón de veces de Google Play.
[27] La versión existente por defecto de la app "Google Play Store" es la 4.5.10.

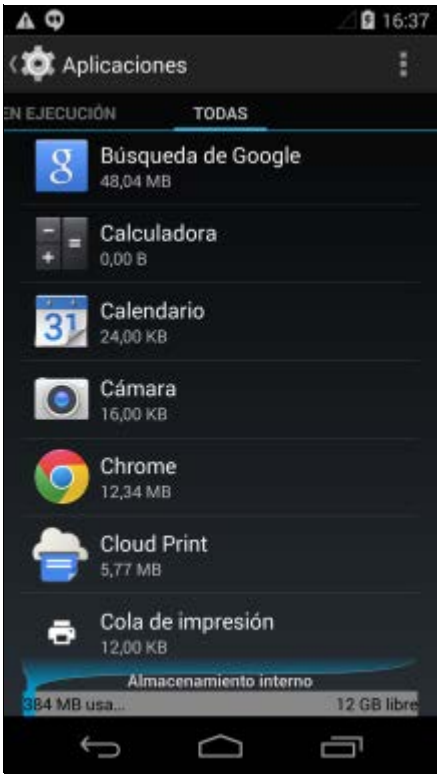
154. A través del botón "Ver todo" (que pasará a denominarse "Ocultar" una vez pulsado) se puede obtener la lista completa de permisos solicitados por la app, incluyendo los permisos considerados menos relevantes por Google:

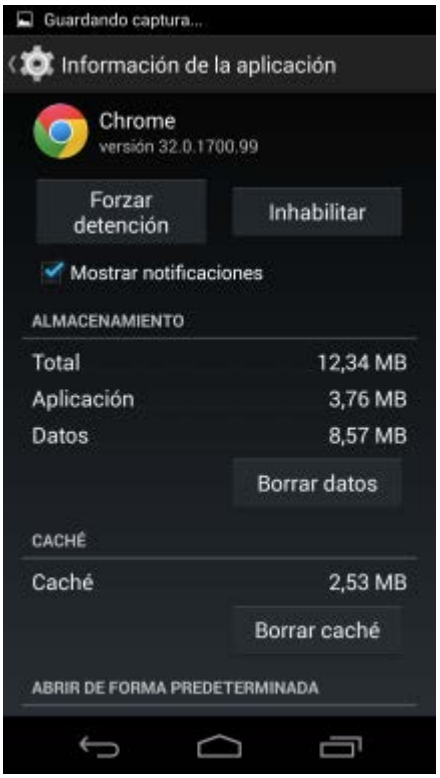


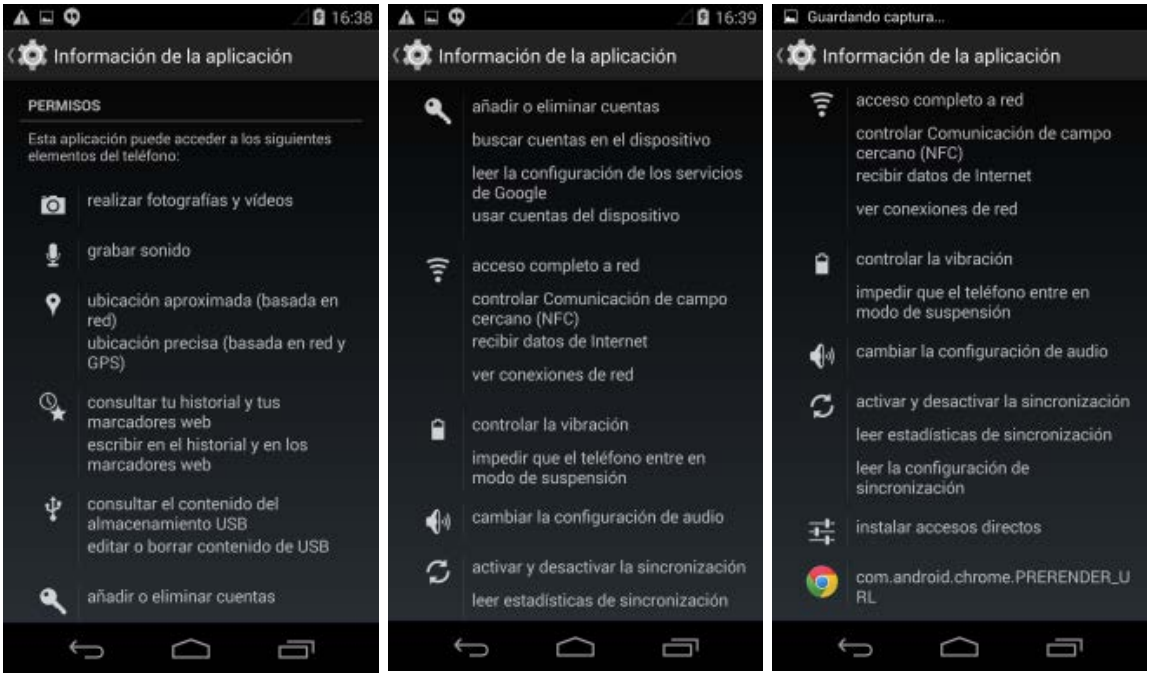
155. Mediante la selección de cualquiera de los permisos es posible obtener una descripción breve sobre su propósito:



156. Una vez la app ha sido instalada, es posible ver los permisos de los que hace uso desde el menú "Ajustes [Dispositivo] - Aplicaciones", seleccionando la app de una de las listas disponibles: Descargadas, En Ejecución, o Todas. En la parte inferior de la pantalla de información de la app se encuentra la lista de permisos empleados (por ejemplo, de la app "Chrome", navegador web por defecto en Android 4.4 (KitKat), versión 32.0.1700.99):

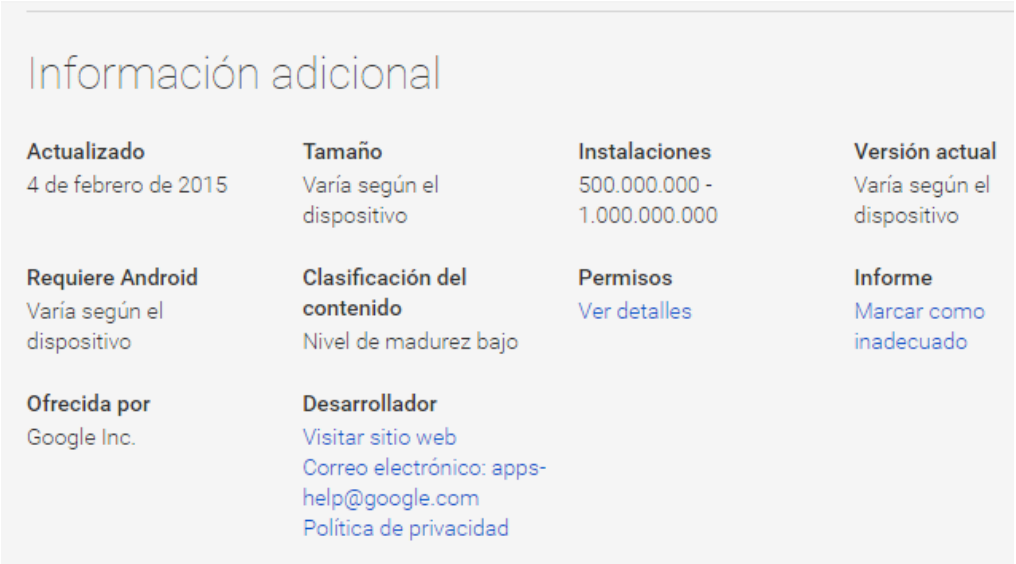




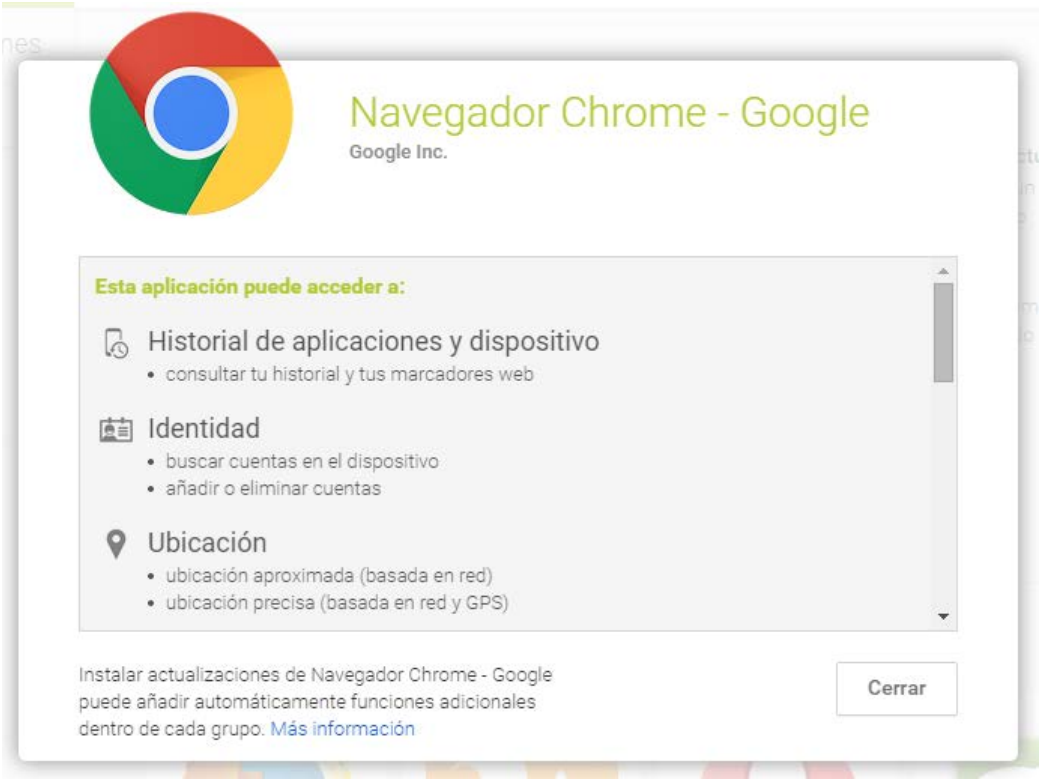


157. Por defecto, las apps no disponen de ningún permiso. Si durante la instalación una app no solicita ningún permiso no quiere decir que (debido a vulnerabilidades en Android) no pueda llevar a cabo acciones que afecten a la privacidad del usuario [Ref.- 56], por lo que el usuario debe evaluar minuciosamente la instalación de nuevas apps incluso cuando éstas parecen no requerir ningún permiso.

158. Los permisos requeridos por una app también están disponibles a través de la página web con su descripción en Google Play, que puede ser consultada antes de su instalación, y en concreto, a través de la sección de "Información adicional" y el apartado "Permisos: Ver detalles" (el ejemplo inferior hace uso de nuevo de la app Chrome[28]):



[28] https://play.google.com/store/apps/details?id=com.android.chrome&hl=es



159. Un elevado porcentaje del código dañino (o malware) para Android se distribuye utilizando el código de otras aplicaciones móviles legítimas, que son modificadas y publicadas de nuevo en el mercado oficial de aplicaciones, Google Play.

160. En otros casos, la app fraudulenta no incorpora ningún código dañino durante la instalación, y éste es añadido al dispositivo móvil posteriormente, en uno de los habituales procesos de actualización de las apps. Este proceso puede hacer uso de vulnerabilidades en Android que no requieren de aprobación por parte del usuario para la instalación de la nueva funcionalidad del código descargado, tal como demostró Jon Oberheide con "RootStrap" en el 2010 [Ref.- 87], ejecutando código nativo ARM fuera de la máquina virtual Dalvik (descrita posteriormente).

161. Mediante técnicas de ingeniería social es también posible instar al usuario a realizar la actualización de una app maliciosa [Ref.- 124].

162. Se recomienda por tanto ser precavido y evaluar la reputación y los permisos requeridos por el software antes de proceder a instalar cualquier app en el dispositivo móvil.

163. Por otro lado, debe tenerse en cuenta que si una actualización asociada a una app ya instalada requiere disponer de nuevos permisos no solicitados y aprobados por el usuario durante la instalación inicial de la app, el usuario será consultado de nuevo para aprobar los nuevos permisos requeridos por la actualización (ver apartado "5.22.5. Actualización de apps en Android"), al menos en versiones previas de Android, debido a ciertas particularidades y novedades en el modelo de permisos descritas a continuación.

5.2.2 PERMISOS SIMPLIFICADOS Y GRUPOS DE PERMISOS DE GOOGLE PLAY

164. En relación a los permisos de Android, Google introdujo una actualización mediante los servicios de Google Play y la app "Play Store" en junio de 2014, en concreto en la versión 4.8.19[29] de "Play Store" (o "Google Play Store"), creando los permisos simplificados (o grupos de permisos) de Android.

165. En lugar de mostrarse a través de Google Play, como en versiones previas, los permisos individuales solicitados por cada app, estos se han simplificado y agrupado en función de las capacidades o funciones específicas a las que está asociado cada uno de los permisos, añadiéndose un icono descriptivo asociado, y creándose grupos de permisos relacionados entre sí.

166. El objetivo de esta modificación era simplificar el interfaz gráfico de usuario (GUI) asociado al modelo de permisos de Android, de forma que los usuarios puedan entender más fácilmente qué tipo de capacidades son requeridas por una app en el momento de su instalación. Aproximadamente se han agrupado unos 150 permisos individuales en una docena de categorías o grupos de permisos.

167. Los grupos de permisos, a su vez, son ordenados por criticidad o relevancia, en base a los criterios de Google, mostrándose en la parte superior los más relevantes y disponiéndose de una categoría "Otros" en la parte inferior, que engloba el resto de permisos solicitados y no agrupados previamente en los permisos principales [Ref.- 160]. Sin embargo, esta categoría adicional puede incluir también permisos relevantes desde el punto de vista de seguridad, como por ejemplo el acceso a los interfaces Bluetooth y NFC, o la capacidad de poder escribir en el historial y en los marcadores o favoritos web.

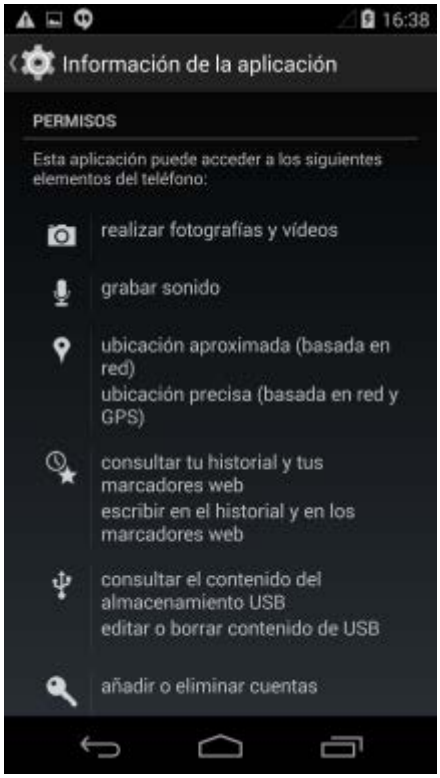
168. Asimismo, en el caso de las apps de terceros que definen sus propios permisos, estos también son englobados dentro de la categoría "Otros".

169. Desde el interfaz de usuario, durante el proceso de instalación de la app, es posible seleccionar los distintos grupos de permisos para ver los permisos individuales solicitados por la app.

170. Igualmente, se pueden consultar los permisos individuales antes de la instalación de una app, desde la app "Play Store" o desde la versión web de Google Play, a través de la sección "Información adicional" se puede seleccionar "Ver detalles" en el apartado de permisos de la app (tal como se describe en el apartado anterior).

171. Asimismo, una vez se ha instalado una app, desde el menú "Ajustes [Dispositivo] - Aplicaciones" es también posible seleccionar la app y en la parte inferior, consultar los permisos individuales solicitados por la misma desde la sección "Permisos":

[29] http://www.androidpolice.com/2014/07/15/google-rolling-out-play-store-v4-8-19-with-paypal-support-simplified-app-permissions-bigger-buttons-and-more-apk-download/#simplified-permission-lists



172. El problema radica en que la implementación de este nuevo modelo de permisos simplificados introduce nuevas vulnerabilidades de seguridad previamente inexistentes.

173. Por ejemplo, una app que requiera disponer del permiso para leer SMS, antes solicitaba únicamente el permiso "READ_SMS ", pero en las últimas versiones solicitará el grupo de permisos "SMS". Al ser instalada, la app obtiene permisos para acceder a todas las capacidades relacionadas con los SMS, incluyendo todos los permisos englobados en dicho grupo, como (potencialmente) el de envío de SMS, aunque el usuario no ha sido consultado (ni ha aprobado) este permiso específicamente [Ref.- 159].

174. Por un lado, las apps que ya han sido instaladas y disponen de ciertos permisos, al recibir la siguiente actualización de la app, obtendrán automáticamente acceso al grupo completo de permisos asociados a cada uno de los permisos individuales que ya disponían. Como resultado, obtendrán automáticamente acceso a muchos más permisos de los que solicitaron inicialmente durante su instalación.

175. Por otro lado, los grupos de permisos contienen tanto permisos menos relevantes desde el punto de vista de seguridad, como permisos más críticos que son habitualmente utilizados por software malicioso. Por ejemplo, apps que solicitan el permiso de los servicios de localización o ubicación, podrán situar la posición del dispositivo móvil tanto de forma aproximada como más precisa a través del módulo GPS, apps que sólo requerían consultar el listado o registro de llamadas podrán realizar llamadas (incluso sin la intervención del usuario), y apps que solicitaban poder leer contenidos de la tarjeta SD podrán escribir también en ella o incluso formatearla.

176. Asimismo, por ejemplo, una app con funcionalidad de linterna (*flashlight*), que previamente requería del permiso para activar el *flash* (o led) de la cámara, al estar este permiso englobado dentro del grupo "Cámara", ahora también dispondrá de permisos para hacer fotografías, o grabar vídeo y audio.

177. Por último, esta actualización del modelo de permisos de Android otorga por defecto el permiso (existente previamente) de acceso completo a Internet a cualquier app. Es decir, el permiso de acceso a Internet ha sido eliminado de manera efectiva, ya que aunque los desarrolladores de apps tienen que seguir declarando que la app requiere dicho permiso, los usuarios no verán la solicitud de este permiso durante el proceso de instalación de la app (en ocasiones se muestra en las vistas detalladas de permisos englobado dentro de la categoría "Otros"). Asimismo, las apps que no disponían del permiso anteriormente, lo pueden obtener automáticamente y sin la aprobación del usuario en la siguiente actualización de la app.

178. Se recomienda por tanto analizar minuciosamente cada uno de los permisos individuales solicitados por las apps durante el proceso de instalación o incluso antes, ignorando la simplificación en grupos de permisos realizada por Google Play

179. Adicionalmente, se recomienda llevar a cabo este mismo análisis minucioso para cada una de las actualizaciones recibidas para las apps ya instaladas en el dispositivo móvil, habiendo deshabilitado previamente las actualizaciones automáticas de las apps (ver apartado "5.22.6. Actualizaciones automáticas de las apps"), con el objetivo de evitar que una actualización de cualquier app adquiera nuevos permisos sin solicitárselos al usuario.

180. Por último, se debe asumir que actualmente cualquier app de Android dispone de capacidades plenas para conectarse y acceder a Internet.

181. Debe tenerse en cuenta que la simplificación del interfaz de usuario para la aprobación de los permisos requeridos por una app sólo afecta a las apps instaladas desde Google Play. La instalación de apps directamente mediante su fichero ".apk" asociada todavía mostrará la lista individualizada de permisos, qué deberá ser aprobada por el usuario.

182. Se dispone de más información sobre los grupos de permisos, así como de los permisos individuales englobados en cada grupo, su propósito y capacidades, en la documentación oficial de Google [Ref.- 160].

5.2.3 SANDBOX DE EJECUCIÓN DE LAS APPS

183. Las apps en Android ejecutan de forma independiente en su propio entorno de ejecución o *sandbox*[30] [Ref.- 16]. Cada aplicación móvil (o app) está asociada a un usuario de sistema operativo diferente.

184. En el momento de su instalación, Android asigna a cada app un identificador de usuario único (user ID y group ID, ID en adelante) a nivel de sistema operativo, y asocia todos los ficheros de la app a dicho ID. De esta forma, sólo la app tendrá acceso a sus ficheros asociados.

185. El ID es asignado y gestionado por Android y las apps no tienen conocimiento del mismo.

186. Excepcionalmente una app puede crear datos (directorios y ficheros) y asignarles permisos de lectura y/o escritura globales, de forma que cualquier otra app pueda acceder a ellos.

187. Cada app ejecutada es un proceso (Linux) independiente a nivel de sistema operativo. El proceso es iniciado cuando cualquiera de los componentes de la app necesita ejecutarse, y es finalizado al no utilizarse más la app o durante las tareas específicas de gestión (y liberación) de memoria del sistema operativo.

[30] https://source.android.com/devices/tech/security/index.html

188. Cada proceso tiene asignada su propia máquina virtual (*Virtual Machine* o VM), por lo que el código de cada app ejecuta de manera aislada al resto de apps.

189. Las apps pueden compartir datos con otras apps a través de la compartición del un mismo ID, y acceder a servicios del sistema operativo mediante la solicitud de permisos para interactuar con componentes y datos del sistema, como la lista de contactos del usuario, los mensajes SMS, la tarjeta de memoria externa, la cámara, el interfaz Bluetooth, disponer de acceso a Internet, el interfaz Wi-Fi, poder realizar llamadas de voz, etc.

190. La lista de permisos disponibles en Android está disponible en la definición del manifiesto o *manifest* (descrito posteriormente) donde se especifican todos los permisos requeridos [Ref.- 23].

191. Las apps que comparten un mismo ID tienen acceso a los mismos ficheros, pueden ejecutar en el mismo proceso y compartir la misma máquina virtual. Para ello deben haber sido firmadas con el mismo certificado digital por su desarrollador, y desde el punto de vista de seguridad, podrían considerarse la misma app.

192. Las apps de Android pueden estar constituidas por diferentes componentes, que permiten la interacción de la app con el sistema y con el usuario, existiendo cuatro tipos de componentes: actividades, servicios, proveedores de contenidos y receptores de anuncios o eventos (*broadcast*) [Ref.- 16].

193. Los mensajes asíncronos de notificación o solicitud de petición entre componentes (de la misma o entre distintas apps) para que se lleve a cabo una acción se denominan *intents*.

194. Cada app de Android dispone de un fichero de definición, o *manifest* ("AndroidManifest.xml") [Ref.- 18], que contiene información sobre los diferentes componentes que constituyen la app. Adicionalmente, el *manifest* incluye los permisos que requiere la app (por ejemplo, acceso a Internet, lectura de la lista de contactos, etc.), las librerías (o APIs, *Application Programming Interface*) empleadas por la app, tanto de sistema como externas (ej. librería de Google Maps), o los elementos o capacidades hardware y software empleados por la app (ej. cámara, interfaz Bluetooth, pantalla táctil, etc.).

195. Estos requisitos hardware y software pueden ser empleados para decidir en qué dispositivos móviles puede instalarse y ejecutar una app en función de sus necesidades, principalmente desde Google Play. Los requisitos pueden ser definidos como necesarios o requeridos, u opcionales, en cuyo caso la app podrá ser instalada pero no hará uso de la funcionalidad asociada al requisito no disponible, como por ejemplo, la cámara.

196. Adicionalmente a los permisos estándar [Ref.- 23], existen una serie de permisos que requieren disponer de un nivel de protección elevado (protectionLevel) y que están disponibles únicamente para las apps existentes en la imagen de sistema de Android o que han sido firmadas con los mismos certificados que éstas [Ref.- 102].

197. Las librerías de sistema, denominadas API Level [Ref.- 19], e identificadas por su número o versión, están asociadas a la versión de Android. Por ejemplo, la API Level 19 corresponde a la versión 4.4 de Android (KitKat).

198. Adicionalmente al código, las apps disponen de recursos (definidos mediante ficheros XML) asociados principalmente a la parte visual o interfaz gráfico de la app, es decir, imágenes, ficheros de audio, contenidos en diferentes idiomas, etc.

199. Con el objetivo de incrementar el modelo y los mecanismos de seguridad disponibles en Android por defecto, la NSA publicó en enero de 2012 una versión de Android restringida,

denominada SE Android, y equivalente en filosofía y funcionalidad a SE Linux para las plataformas Linux estándar [Ref.- 103].

200. Security Enhanced (SE) Android, SE Android, mejora la seguridad de Android limitando el daño que puede infringir un código dañino, o una potencial vulnerabilidad de seguridad, que afecte al dispositivo móvil, así como añadiendo capacidades para aislar las apps y ficheros entre sí.

201. Posteriormente, las capacidades de SE Android fueron integradas en la plataforma móvil estándar, tal como se describe en el apartado "5.2.5. SELinux en Android".

5.2.4 FIRMA DIGITAL DE APPS EN ANDROID

202. Para que una app sea considerada válida y pueda ser distribuida oficialmente a través de Google Play debe haber sido firmada digitalmente por su desarrollador [Ref.- 28].

203. Sin embargo, Android no realiza ninguna verificación adicional sobre la seguridad de la app (salvo las especificadas en el apartado "5.23.4. Verificación de seguridad de las apps") o la firma digital, salvo comprobar la fecha de expiración del certificado asociado a la firma en el momento de la instalación de la app[31], permitiéndose certificados auto-firmados y no generados o validados por ninguna autoridad certificadora.

204. Por tanto, la firma digital de las apps en Android no evita que las mismas contengan vulnerabilidades de seguridad o código malicioso. La firma únicamente permite vincular (teóricamente) la app a su desarrollador, asegura su integridad frente a modificaciones, se emplea para las actualizaciones de la app, verificando que el nuevo código proviene del mismo desarrollador, y en algunos escenarios como la compartición del ID entre apps, define el nivel de privilegios de ejecución de la app con respecto a otras apps, permitiéndolas compartir datos entre sí, es decir, estableciendo relaciones de confianza entre apps.

205. La vinculación entre la app y el desarrollador no ofrece fiabilidad desde el punto de vista de seguridad, ya que al permitirse emplear certificados auto-firmados, los mismos pueden contener información que no está asociada al desarrollador real de la app. Es decir, la firma de una app no permite necesariamente identificar a su desarrollador real.

206. Las apps de Android se distribuyen a través de ficheros APK (*Android PacKage*), una extensión del formato de paquetes Java JAR. Por tanto, hacen uso de capacidades similares a las existentes para firmar ficheros JAR para la firma de los paquetes o ficheros APK [Ref.- 45].

207. La firma de apps no es empleada (como si puede ser en caso en aplicaciones Java) para la verificación de la integridad (es decir, la firma) de segmentos o porciones de código durante la ejecución de la app. Los controles en tiempo de ejecución se basan en los UIDs/GIDs de los procesos asociados a la app [Ref.- 26].

208. La firma de las apps es también empleada para permitir la instalación de actualizaciones de las apps, confirmándose que provienen del mismo desarrollador.

209. Las apps de sistema han sido firmadas empleando un conjunto de claves asociadas a la plataforma o sistema, pertenecientes a Google (en el caso de las apps por defecto de Android y de los dispositivos móviles Nexus) o a los fabricantes de dispositivos móviles u operadores de telefonía móvil (en el caso de los dispositivos móviles con una versión

[31] Existen referencias confirmando la posibilidad de instalar apps incluso con certificados expirados [Ref.- 26].

modificada por estos de Android, incluyendo las apps propietarias que estos han incluido).

5.2.5 SELINUX EN ANDROID

210. El modelo de seguridad de Android se basa parcialmente en la utilización de contenedores (o *sandboxes*) para cada aplicación móvil (o app). La implementación previa a la versión 4.3 de Android empleaba un identificador de usuario (UID) único de Linux, generado en el momento de la instalación de la app, para restringir el entorno de ejecución de cada app. Sin embargo, a partir de la versión 4.3 de Android, se emplea también SELinux (Security-Enhanced Linux) para restringir los límites y capacidades asociadas a una app y a su contenedor [Ref.- 140].

211. SELinux proporciona soporte en Android para un modelo de seguridad conocido como MAC (Mandatory Access Control), frente al modelo de seguridad estándar y tradicional de Unix/Linux, conocido como DAC (Discretionary Access Control), junto a la definición asociada de políticas de seguridad.

212. Como ya se mencionó brevemente en el apartado "4. Entorno de aplicación de esta guía", las capacidades MAC de SELinux en Android se pueden emplear en todos los procesos, tanto los asociados a las apps como los procesos de sistema que ejecutan como root, pero su implementación es dependiente de la versión de Android [Ref.- 139] [Ref.- 140].

213. En Android 4.3 se hace uso de SELinux en modo permisivo o *permissive mode*, donde únicamente las acciones no legítimas son registradas por el kernel, pero no bloqueadas.

214. En Android 4.4 se hace uso de SELinux en modo obligatorio o *enforcing mode* parcialmente, es decir, sólo para un conjunto crítico de procesos o dominios de sistema (installd, netd, vold y zygote), en el que todas las acciones no legítimas son bloqueadas y registradas por el kernel. Para el resto de procesos o dominios, SELinux en Android 4.4 sigue actuando en modo permisivo, como en el caso de Android 4.3.

215. En Android 5.0 se hace uso de SELinux en modo obligatorio o *enforcing mode* globalmente o completo (*full enforcement*), es decir, tanto para el conjunto crítico de procesos de sistema (ya protegidos en Android 4.4), como para el resto de procesos (con más de 60 dominios).

5.2.6 APP OPS

216. "Apps Ops" es un sistema granular de control o gestión de los permisos de las apps en Android, oculto por defecto, y que fue introducido por Google en Android 4.3 [Ref.- 125].

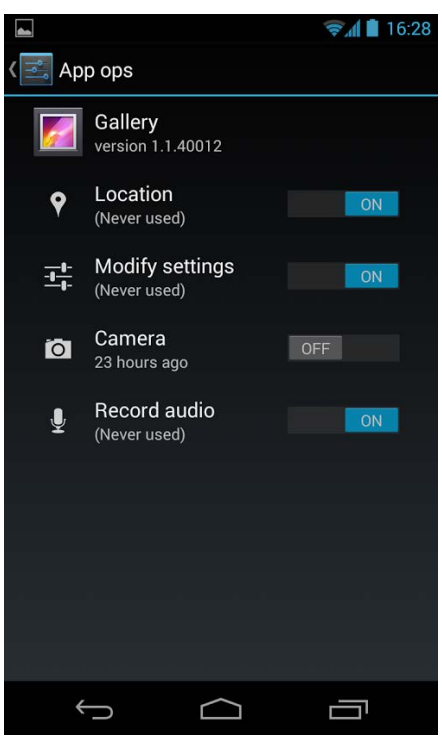
217. La principal ventaja de "App Ops" era que puede ser usado para gestionar los permisos tras la instalación de cualquier app, en lugar de tener que aceptar o denegar los permisos en el momento de la instalación de la app, tal y como ocurre por defecto en Android. Esta funcionalidad permite revocar permisos individualmente y para cada app.

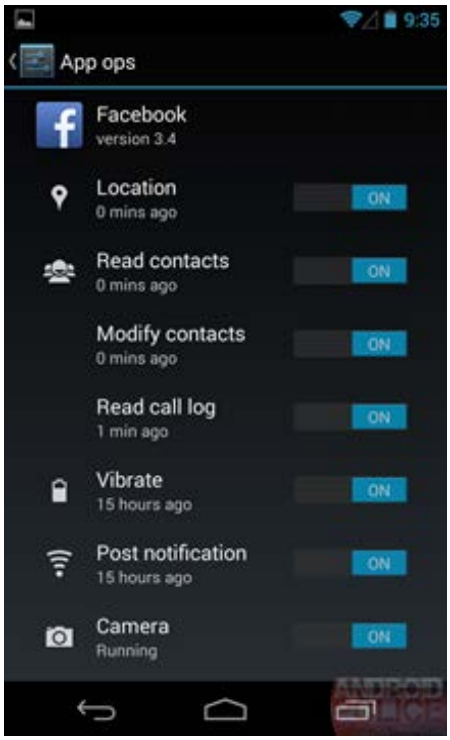
218. Sin embargo, sólo es posible configurar cada permiso una vez que éste ha sido utilizado, en lugar de proporcionar la lista completa de permisos de la app, por ejemplo, desde su fichero "AndroidManifest.xml". Por otro lado, no se genera ninguna notificación hacia el usuario cuando un permiso solicitado por una app es denegado, por ejemplo, explicando el motivo de porqué no es posible hacer uso de dicho permiso.

219. Para poder hacer uso de "App Ops" era necesario crear un acceso directo personalizado que apuntase a la actividad asociada a "Ajustes - App Ops". La creación de este acceso

directo se puede llevar a cabo a través de otra app creada específicamente para este propósito, como por ejemplo la app llamada "AppOps" [Ref.- 129] (entre otras[32]).

220. "App Ops" proporcionaba controles granulares para permisos clasificados en diferentes categorías, como los servicios de localización, permisos personales, de mensajería o del dispositivo. Por ejemplo, permitía habilitar y deshabilitar la modificación de los ajustes, la cámara, la posibilidad de grabar audio del micrófono del dispositivo móvil, notificaciones, vibraciones del teléfono, lectura y modificación de los contactos, lectura del registro de llamadas, etc:





221. "App Ops" permitía también ver la última vez que cada permiso había sido utilizado.

222. Posteriormente, en Android 4.4, "App Ops" seguía disponible y añadía capacidades para gestionar más permisos (como por ejemplo la capacidad de una app de despertar al dispositivo móvil, "keep awake") y una nueva categoría asociada a contenidos multimedia [Ref.- 126].

223. Sin embargo, finalmente "App Ops" fue eliminada por Google en la versión 4.4.2 de Android [Ref.- 158], confirmando su carácter experimental y el riesgo de que algunas apps dejaran de funcionar correctamente (ya que las apps esperan disponer de los permisos solicitados una vez han sido instaladas y aprobadas por el usuario, en base al modelo general de permisos de Android).

224. Actualmente, sólo puede hacerse uso de "App Ops" en dispositivos móviles Android *rooteados* (por ejemplo, mediante un módulo Xposed denominado AppOpsXposed[33]).

[32] https://play.google.com/store/apps/details?id=com.pixelmonster.AppOps&hl=en
[33] http://www.howtogeek.com/177915/how-to-restore-access-to-app-ops-in-android-4.4.2/

5.3 GESTIÓN EMPRESARIAL DE DISPOSITIVOS MÓVILES BASADOS EN ANDROID

225. Las estrategias y soluciones empresariales de gestión de dispositivos móviles, conocidas como MDM en inglés (*Mobile Device Management*), constituyen un elemento fundamental para gestionar el nivel de riesgo y los mecanismos de seguridad en todas las organizaciones y compañías que pretendan integrar el uso de estos dispositivos en sus actividades diarias.

226. Se dispone de información detallada sobre las soluciones de gestión empresarial de dispositivos móviles o MDM en la guía "CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management)" [Ref.- 131].

227. Google proporciona capacidades empresariales para la gestión de dispositivos móviles basados en Android a través de la plataforma Google Apps [Ref.- 12], accesibles desde un navegador web y que no requiere el despliegue de servidores dedicados para este propósito, al emplearse los servicios de Google "en la nube".

228. Desde la versión 2.2 de Android los administradores de un dominio Google Apps (ediciones *Premier* o *Business*, *Government* o *Education*) disponen de capacidades para gestionar políticas de seguridad sobre los dispositivos móviles, incluyendo [Ref.- 88]:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado (ver apartado "5.8. Eliminación de datos del dispositivo móvil").

  Nota: este proceso es equivalente a la opción "Restablecer datos de fábrica" disponible desde el menú "Ajustes - Copia de seguridad [Datos Personales]".

- Forzar la solicitud de un código de acceso al dispositivo móvil.
- Definir la longitud mínima de los códigos de acceso.
- Forzar la utilización de letras y números en las contraseñas de acceso.
- Bloquear el dispositivo móvil tras un periodo de inactividad, cuya duración puede ser también definida en la política de seguridad.

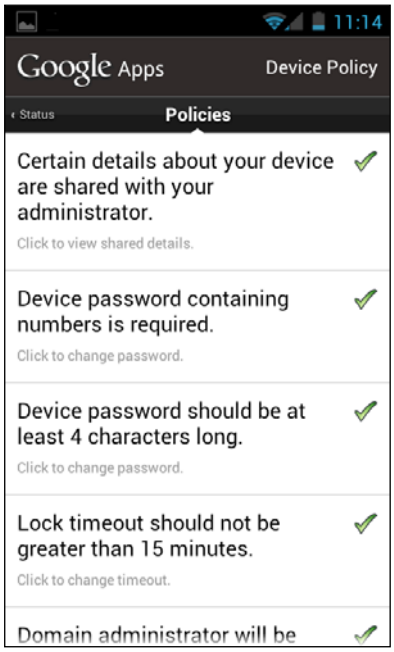
229. Adicionalmente, los usuarios de los terminales pueden de forma remota restaurar (o resetear) el código de acceso (ver apartado "5.4.12. Restauración del código de acceso"), hacer que suene el dispositivo móvil, bloquear el mismo, localizar su ubicación y llevar a cabo el borrado remoto de los datos (si la opción ha sido habilitada por el administrador).

230. Para poder implantar estas políticas de seguridad es necesario que el dispositivo móvil disponga de la app "Google Apps Device Policy", disponible de forma gratuita en Google Play [Ref.- 13].

231. La versión 2.0 (o superior) de la app "Google Apps Device Policy" permite adicionalmente a los administradores definidos en Google Apps incluir como requisito de la política de seguridad el cifrado de los datos de las *tablets* basados en Android 3.0 o los *smartphones* en la versión 4.0 (ver apartado "5.6.1. Cifrado del dispositivo móvil"), opción disponible desde el panel de control asociado en Google Apps [Ref.- 94].

232. El acceso a la gestión de políticas para los usuarios empresariales de Google Apps (Business, Education y Government) está disponible desde el panel de control de Google Apps, y en concreto desde la pestaña "Service Settings" y la opción "Mobile".

233. Las políticas también están disponibles desde el propio dispositivo móvil empleando el menú "Device Policy" de la app "Google Apps Device Policy" [Ref.- 61]:



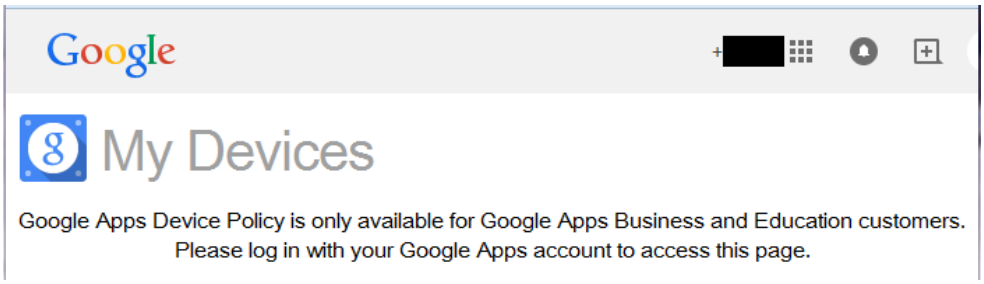
234. La capacidad de borrado remoto de datos sólo afecta al almacenamiento local del dispositivo móvil, no siendo posible actualmente eliminar también los datos de la tarjeta de almacenamiento externa conectada al dispositivo móvil (en caso de existir ésta).

235. Una vez se establecen las políticas de seguridad a nivel empresarial y se dispone de la app instalada en los dispositivos móviles a gestionar, un usuario podría desinstalar la app. Sin embargo, el administrador puede configurar el entorno de gestión para que en ese escenario no sea posible sincronizar ningún dato entre el dispositivo móvil y el entorno corporativo (e-mails, contactos, eventos de calendario o fotografías) desde el momento en que se lleve a cabo la desinstalación de la app.

236. El acceso a la gestión empresarial del dispositivo móvil por parte de los usuarios finales, y no de los administradores del dominio asociados en Google Apps, puede realizarse mediante la sección "Mis dispositivos" (o "My devices"), disponible en la URL "https://www.google.com/apps/mydevices", de la página web de Google Apps.

237. Desde "Mis dispositivos", un usuario o el administrador de la organización, puede bloquear remotamente su dispositivo móvil perdido o robado, cambiar el código de acceso, hacer sonar el dispositivo móvil, localizarlo, o borrar sus datos remotamente (*wipe*) [Ref.- 61].

238. Sin embargo, el acceso a "My Devices" por parte de un usuario no asociado a un dominio de Google Apps no está permitido, obteniéndose el siguiente mensaje informativo:



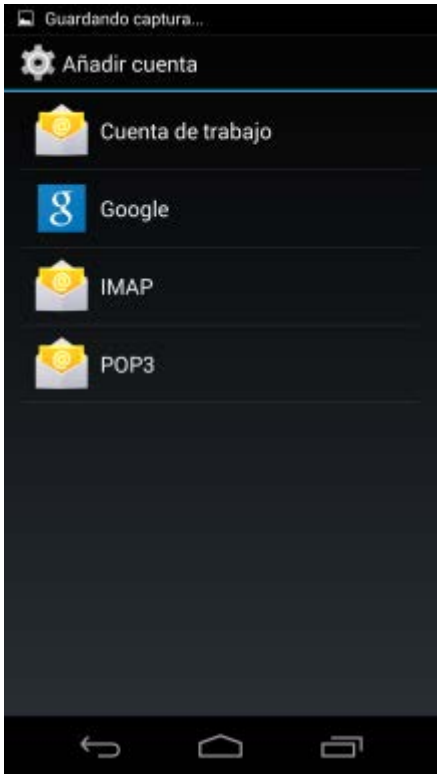
239. Microsoft, a través de Microsoft Exchange ActiveSync, también proporciona capacidades de gestión empresarial de dispositivos móviles Android [Ref.- 38], siendo posible la

aplicación de numerosas políticas de seguridad [Ref.- 36] (no todas ellas descritas en el presente documento), incluyendo:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado.
- Borrado local de los datos del dispositivo móvil (*wipe*), en caso de realizar un número determinado de intentos de acceso incorrectos.
- Forzar la solicitud de un código de acceso al dispositivo móvil.
- Definir la longitud mínima de los códigos de acceso.
- Definir la complejidad de las contraseñas de acceso (mínimo número de caracteres no alfabéticos).
- Forzar la utilización de letras y números en las contraseñas de acceso.
- Prevenir la reutilización de las últimas "N" contraseñas únicas (histórico de contraseñas).
- Definir el periodo de expiración de la contraseña, obligando al usuario a cambiarla (o sino el correo electrónico no se sincronizará con el servidor Exchange).
- Bloquear el dispositivo móvil tras un periodo de inactividad, cuya duración puede ser también definida en la política de seguridad.
- Definir si los dispositivos móviles que no soporten todas las opciones definidas en la política de seguridad (no sólo algunas de ellas) pueden sincronizar información con el servidor Exchange.
- Permitir la descarga de ficheros adjuntos al dispositivo móvil, y definir el tamaño máximo de los adjuntos.
- Deshabilitar la cámara (y muchos otros componentes e interfaces hardware).
- Definir si se requiere que el dispositivo móvil haga uso de cifrado completo del dispositivo.

240. Las capacidades disponibles en la política de seguridad dependen de la versión de Android existente en los dispositivos móviles, y de la versión de Microsoft Exchange empleada por la organización (2003, 2007, 2010, 2013..., y la versión de Service Pack (SP) concreta).

241. El dispositivo móvil Android puede ser configurado mediante la creación de una cuenta de Microsoft Exchange ActiveSync desde el menú "Ajustes [Cuentas] - Añadir cuenta - Cuenta de trabajo", siendo necesario proporcionar las credenciales de la cuenta existente, es decir, la dirección de correo electrónico del usuario y la contraseña:



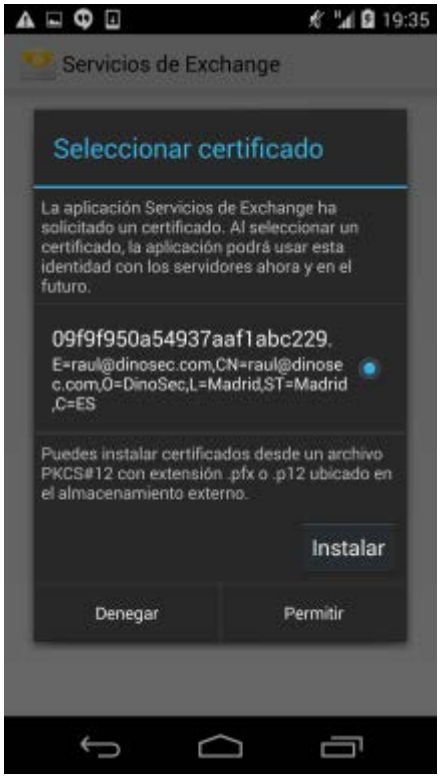
242. Tras pulsar el botón "Siguiente" se debe seleccionar el tipo de cuenta: POP3, IMAP o Exchange. En el caso de Exchange, es necesario facilitar el nombre del servidor Exchange, el puerto y el tipo de seguridad:

243. Para proteger las comunicaciones extremo a extremo entre el dispositivo móvil y el servidor Exchange es necesario habilitar la opción "SSL/TLS" (habilitada por defecto) y no habilitar en ningún caso las opciones "Ninguna" o "SSL/TLS (aceptar todos los certificados)":

Nota: la opción "SSL/TLS (aceptar todos los certificados)" implica que Android aceptaría cualquier certificado digital recibido por parte del servidor Exchange (certificados autofirmados, expirados, o no válidos), permitiendo la realización de ataques *Man-in-the-Middle* (MitM) por parte de un atacante para interceptar y manipular el tráfico intercambiado.

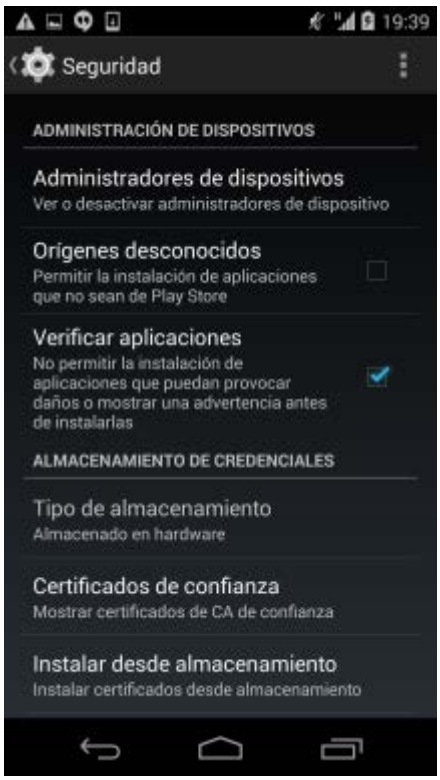
Nota: la gestión empresarial detallada de dispositivos móviles Android mediante Microsoft Exchange y ActiveSync (2003 SP2, 2007 o superior), Microsoft Exchange Online (https://www.microsoft.com/online/exchange-online.aspx) o System Center Configuration Manager (SCCM) 2012, incluyendo su implementación, configuración, e integración con las soluciones Microsoft Exchange está fuera del alcance de la presente guía [Ref.- 36][Ref.- 37].

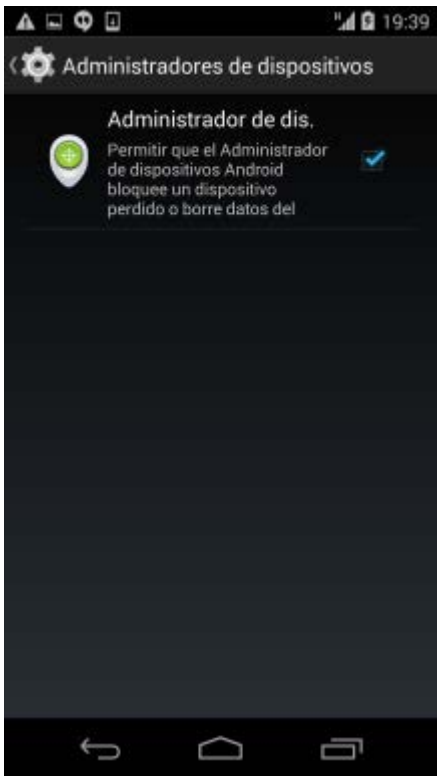
244. Adicionalmente, la configuración de Android permite utilizar un certificado digital cliente para la autentificación del usuario, mediante la opción "Certificado de cliente", que debe haber sido importado previamente en el dispositivo móvil en formato PKCS#12 (al igual que para las redes Wi-Fi o redes VPN, ver apartado "5.14.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi"):



245. Desde la versión 2.2 de Android se permite añadir múltiples cuentas de Microsoft Exchange al dispositivo móvil.

246. Desde la versión de Android 4.4 (KitKat), el administrador de dispositivos Android (*Android Device Manager*) está integrado por defecto en el propio sistema operativo, y disponible a través del menú "Ajustes [Personal] - Seguridad [Administración de Dispositivos] - Administradores de dispositivos":



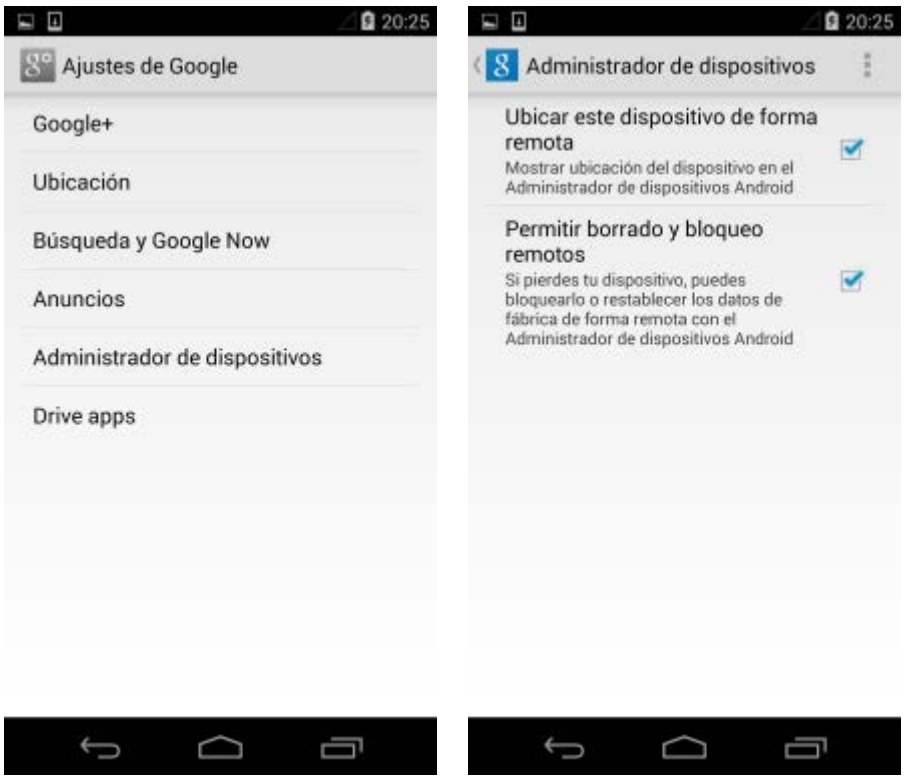


247. Otros dispositivos móviles Android más antiguos, incluso aunque no dispongan de la versión Android 4.4 (KitKat), pueden disponer del administrador de dispositivo Android (aunque no esté habilitado por defecto), ya que el mismo fue introducido por Google en una de las actualizaciones del componente (y app) asociado a los servicios de Google Play[34] (sin ser necesario realizar una actualización de la versión del sistema operativo).

248. En aquellos dispositivos móviles que disponían de Android 4.4.x inicialmente (de fábrica), o que han sido actualizados desde la imagen completa de fábrica de Android 4.4.x, el administrador de dispositivos Android está habilitado por defecto. Sin embargo, aquellos dispositivos que hayan sido actualizados a Android 4.4.x a través de las actualizaciones parciales OTA lo tendrán deshabilitado por defecto.

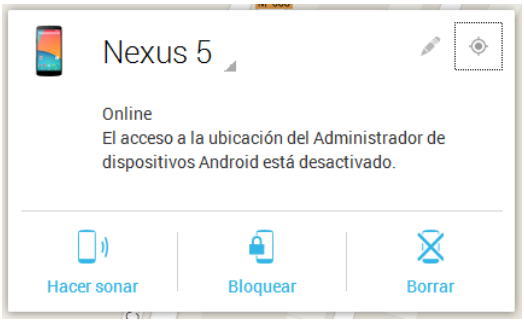
249. En el caso de dispositivos móviles con varios usuarios, únicamente el usuario administrador podrá habilitar o deshabilitar el administrador de dispositivos Android.

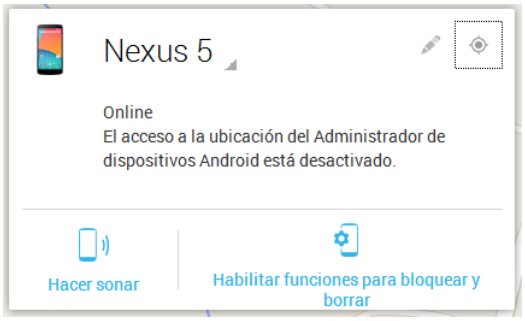
250. Adicionalmente, la app "Ajustes de Google" existente por defecto en Android 4.4 permite, entre otros, modificar las capacidades y configuración del administrador de dispositivos a través de la opción "Administrador de dispositivos". Las opciones de configuración permiten habilitar y deshabilitar individualmente la posibilidad de localizar al dispositivo móvil remotamente ("Ubicar este dispositivo de forma remota"), y de eliminar los datos y bloquear el dispositivo móvil remotamente ("Permitir borrado y bloqueo remotos"):



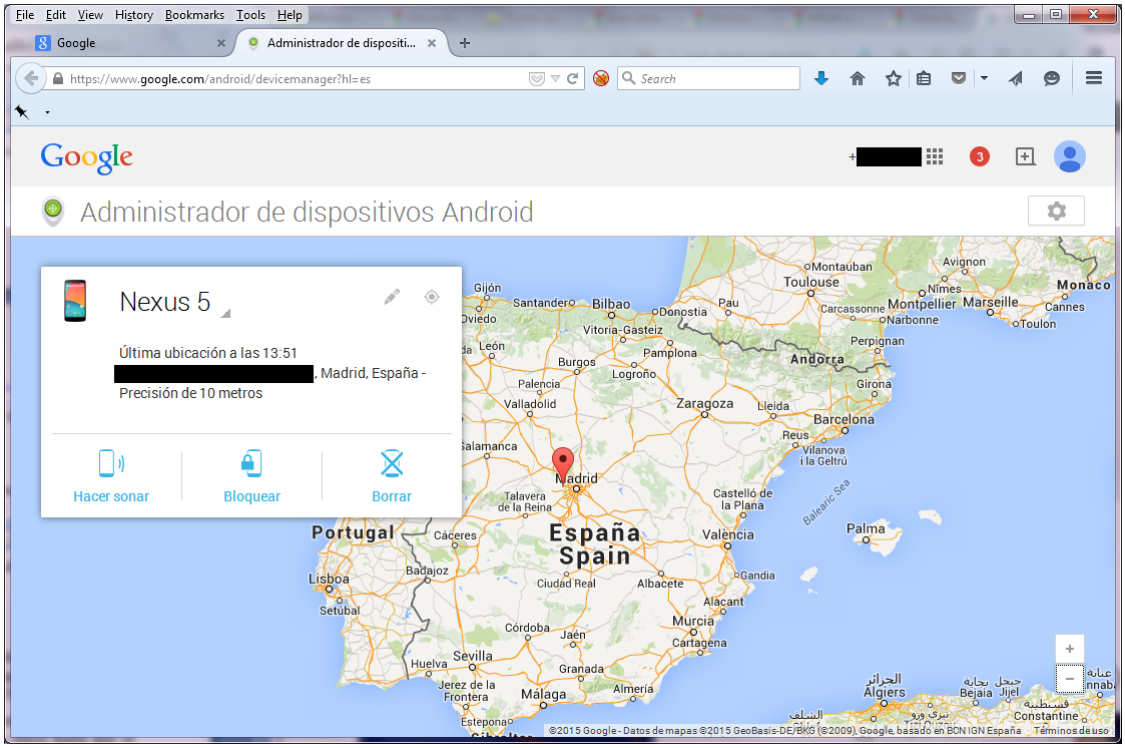
[34] http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/

251. Si se deshabilitan estas opciones, al intentar hacer uso de la ubicación a través del "Administrador de dispositivos Android" (descrito a continuación), se reflejará su estado como desactivado, y en el caso de las funciones de bloqueo, se refleja inmediatamente en el interfaz de usuario:





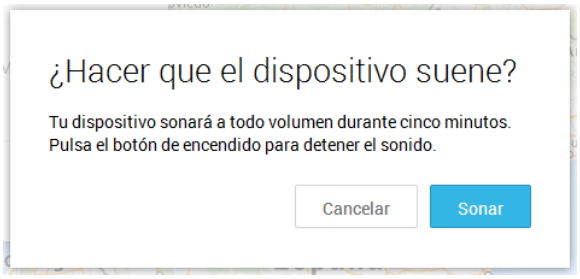
252. El acceso a la gestión del dispositivo móvil por parte de los usuarios particulares, no asociados a un dominio de Google Apps, puede realizarse mediante la sección "Administrador de dispositivos Android" (o *Android Device Manager*), disponible en la URL "https://www.google.com/android/devicemanager?hl=es"[35], o desde la app "Android Device Manager" disponible en Google Play[36]:



[35] https://www.android.com/devicemanager
[36] https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=es

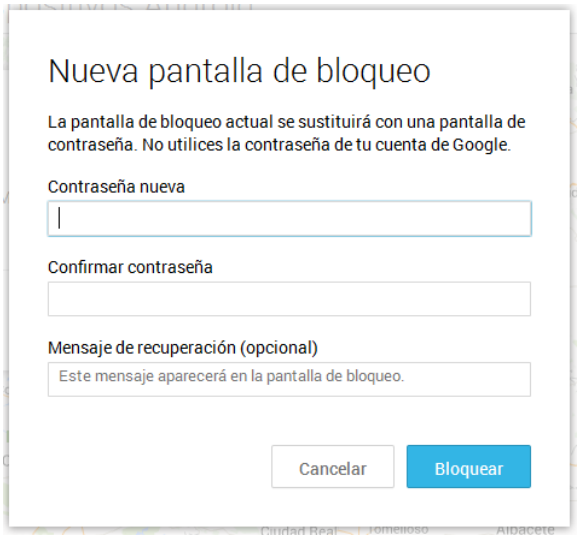
253. Desde este administrador de dispositivos Android un usuario individual puede modificar el nombre identificativo o alias, y hacer sonar el dispositivo móvil, localizar su ubicación, bloquear remotamente el dispositivo móvil, muy útiles si éste ha sido perdido o robado, cambiar el código de acceso, o borrar sus datos remotamente (*wipe*) [Ref.- 39].

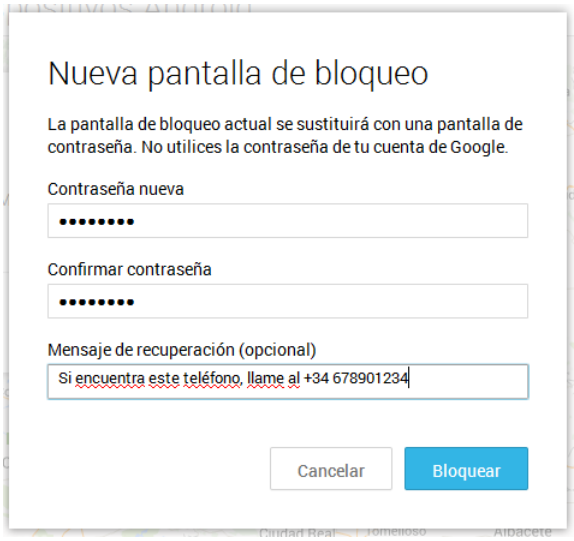
254. La funcionalidad para hacer sonar el dispositivo móvil permite que el dispositivo suene a todo volumen, incluso si estaba en silencio, hasta que se pulse el botón de encendido o la pantalla del dispositivo móvil, con el objetivo de poder localizarlo:



255. La funcionalidad para localizar la ubicación del terminal (habilitada automáticamente al acceder al "Administrador de dispositivos Android" o manualmente mediante el botón circular con una cruceta) permite identificar en Google Maps dónde se encuentra el dispositivo actualmente, o la última vez que se recibió información de su ubicación:

256. La funcionalidad para bloquear remotamente el dispositivo móvil permite establecer un código de acceso, tanto si el dispositivo móvil no disponía de uno previamente (escenario totalmente desaconsejado desde el punto de vista de seguridad), como si ya tenía uno establecido (cambiando su valor de manera efectiva). Adicionalmente se permite al usuario mostrar un mensaje de recuperación en la pantalla de desbloqueo:



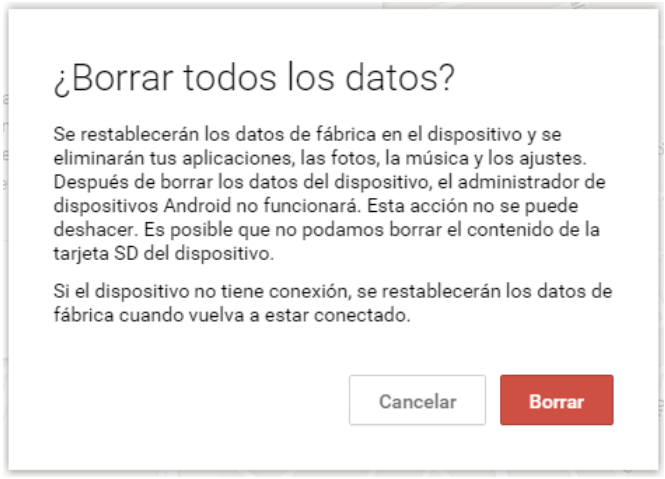


257. Una vez ejecutada la acción, si ésta ha tenido éxito, se recibe confirmación de la operación. Si no ha sido posible contactar con el dispositivo móvil, se informa de que se ha enviado la solicitud. Cuando el dispositivo móvil vuelva a disponer de conectividad de datos, recibirá la petición, y ejecutará la acción. En ese momento se mostrará el mensaje de confirmación[37]:

258. Como resultado, si la acción ha tenido éxito, el teléfono mostrará una nueva pantalla de desbloqueo, con el mensaje especificado previamente (cada vez que se apague la pantalla) y ofreciendo la posibilidad de desbloquear el dispositivo móvil con el nuevo código de acceso especificado:

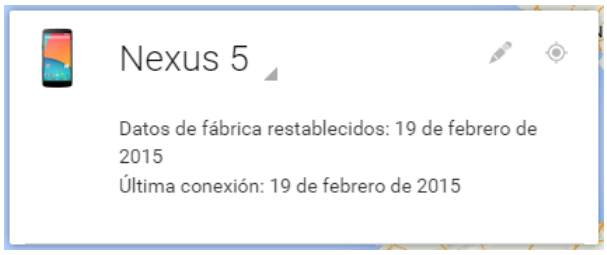
259. La funcionalidad de borrar los datos del dispositivo móvil desde el acceso web al "Administrador de dispositivos Android" permite eliminar todos los datos del terminal remotamente desde la web:

[37] Desafortunadamente, no se ha identificado la existencia de ningún registro (o log) que refleje las diferentes acciones llevadas a cabo, junto a las confirmaciones del terminal, incluyendo una referencia temporal.



260. Una vez ejecutada la acción, mediante el botón "Borrar", si el dispositivo móvil tenía conectividad de datos, se restaurará su configuración de fábrica.

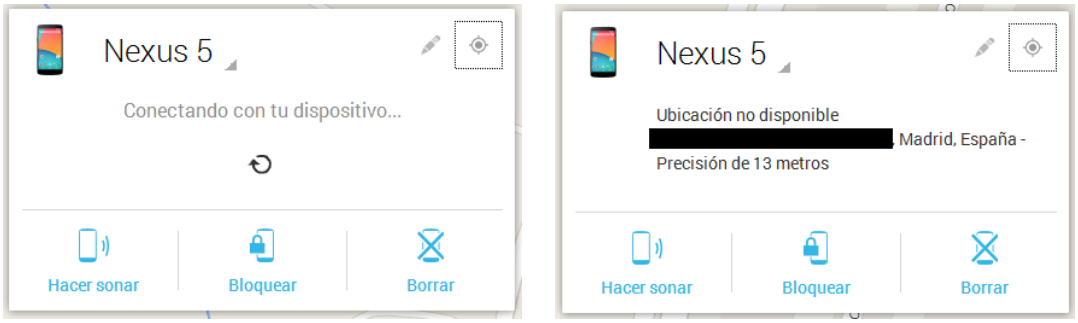
261. La existencia de un mensaje que indica "Datos de fábrica restablecidos", junto a la fecha, no es indicativo de que la operación haya tenido éxito, sino simplemente que ha sido ejecutada y (potencialmente) enviada:



262. Desafortunadamente, tanto si la operación ha tenido éxito como si no, no se recibe confirmación del resultado para su consulta, con el objetivo de que el usuario pueda confirmar que los datos han sido efectivamente eliminados del dispositivo móvil

263. El proceso de eliminación de los datos es equivalente a un *hard reset*, es decir, al restablecimiento del dispositivo móvil a la configuración de fábrica. Durante el proceso además se eliminarán los programas instalados, junto a los datos y a las configuraciones realizadas por el usuario.

264. Si el dispositivo móvil no dispone de conexión de datos, el administrador de dispositivos Android no podrá bloquear o hacer sonar el dispositivo ni borrar sus datos hasta que se establezca una conexión a través de una red Wi-Fi o de la red de datos móviles. Al seleccionar una acción en el administrador de dispositivos Android, ésta se llevará a cabo la próxima vez que el dispositivo móvil vuelva a estar conectado. Lógicamente, el administrador de dispositivos Android no funciona para dispositivos móviles que estén apagados o con el modo avión activo:



5.4 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

265. La posibilidad de disponer de acceso físico al dispositivo móvil, incluso sólo temporalmente, permitiría a un potencial atacante acceder a los contenidos del mismo o hacer uso de los servicios de telefonía móvil disponibles.

266. Para evitar ambos tipos de acceso es posible fijar un PIN (*Personal Identification Number*) o código de acceso tanto en la tarjeta SIM como en el propio dispositivo móvil.

5.4.1 PIN DE LA TARJETA SIM

267. El PIN de la tarjeta SIM bloquea el acceso no autorizado a los servicios y capacidades de telefonía móvil asociados a la propia tarjeta SIM. Si la tarjeta SIM está bloqueada (se desconoce el código PIN), únicamente se permite la realización de llamadas de emergencia (112).

268. Sin embargo, si sólo se establece el PIN en la tarjeta SIM y no en el dispositivo móvil (ver apartado "5.4.2. Código de acceso al dispositivo móvil"), aún es posible para un potencial atacante acceder al terminal directamente, incluyendo sus datos y apps, tras extraer la tarjeta SIM del dispositivo móvil:

269. Si se ha establecido un PIN en la tarjeta SIM, al arrancar el dispositivo móvil no es posible acceder al mismo mediante ningún botón, ya que Android continua solicitando el PIN de la tarjeta SIM para permitir el acceso al terminal, siendo necesario extraer la tarjeta SIM previamente para disponer de acceso al terminal sin introducir el PIN.

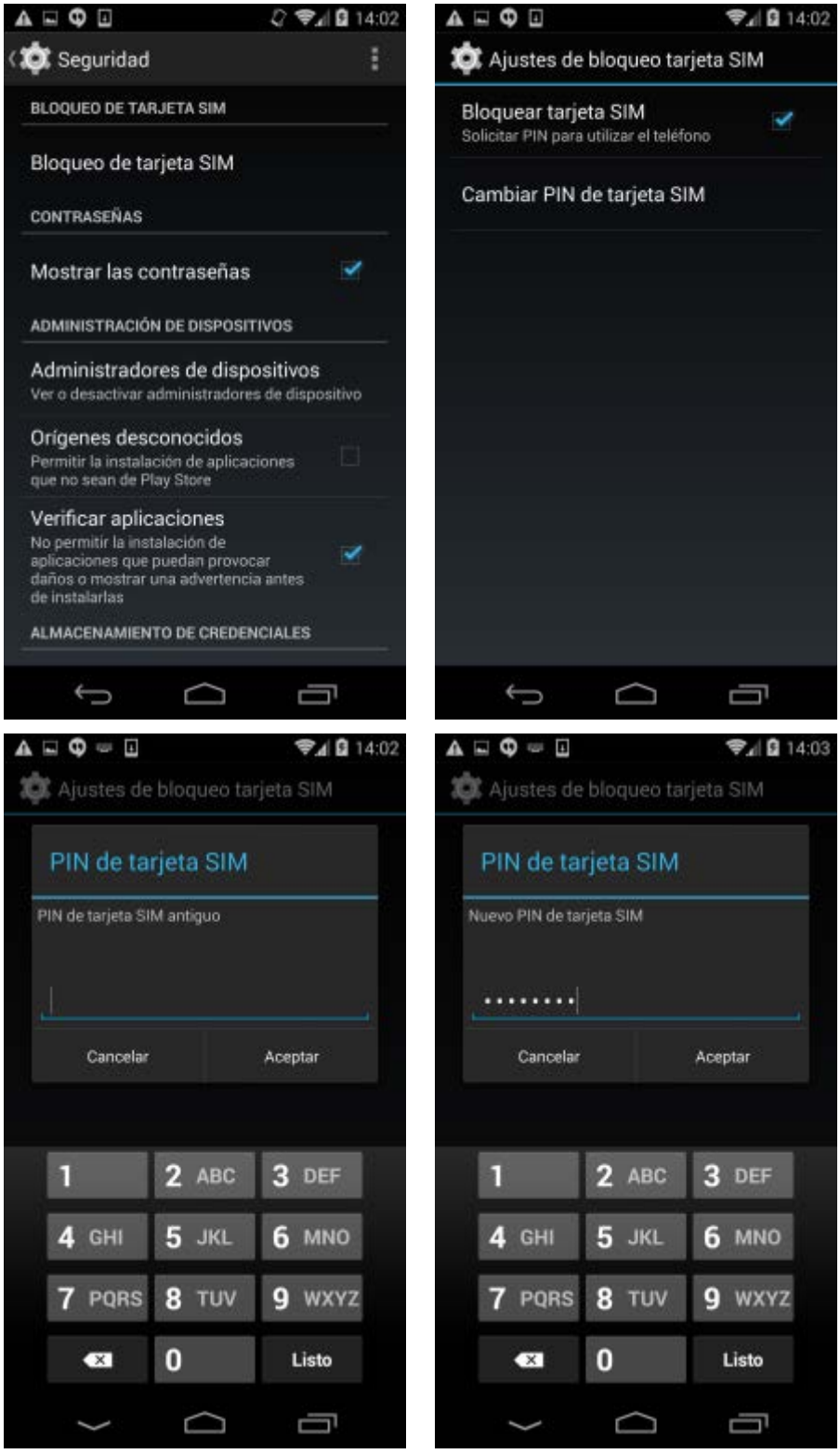
270. La disponibilidad de un PIN por defecto asociado a la tarjeta SIM depende del operador de telefonía móvil, siendo muy habitual que las tarjetas SIM tengan fijado un valor por defecto que es proporcionado en la documentación del contrato del operador de telefonía móvil facilitada al usuario al solicitar sus servicios.

271. El estándar de la industria en la actualidad define un código de 4 dígitos (0-9) como PIN o código de acceso para proteger la tarjeta SIM, sin embargo se recomienda hacer uso de un PIN de mayor longitud, en concreto, de 8 dígitos (longitud máxima permitida).

272. Android permite emplear un PIN de la tarjeta SIM con un valor de 4 a 8 dígitos:

273. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, los operadores de telefonía móvil y fabricantes de dispositivos móviles implementan otros mecanismos para evitar este tipo de ataques, como el bloqueo de la tarjeta SIM tras tres intentos de acceso fallidos. En ese caso, para poder desbloquear la tarjeta SIM es necesario emplear una segunda clave de acceso denominada PUK (*PIN Unlock Key*).

274. Los dispositivos móviles Android permiten forzar la utilización de un PIN para la tarjeta SIM (opción "Bloquear tarjeta SIM"), así como fijar o modificar el PIN asociado a la tarjeta SIM (opción "Cambiar PIN de tarjeta SIM"), a través del menú "Ajustes - Seguridad [Bloqueo de tarjeta SIM] - Bloqueo de tarjeta SIM":



Nota: el menú "Ajustes" empleado y referenciado en numerosas tareas de configuración del dispositivo móvil Android está disponible desde el menú de ajustes rápidos (situado en la barra superior de estado) del dispositivo móvil, o desde el icono del *Launcher* (icono con una matriz de puntos situado en la parte inferior central de la pantalla principal o *Home* de Android).

275. Se recomienda por tanto fijar en la tarjeta SIM la restricción que requiere introducir un PIN para hacer uso de ésta, y modificar el valor por defecto del PIN, fijando el PIN de la tarjeta

SIM con un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111 ó 1234.

276. Debe tenerse en cuenta que cada vez que el dispositivo móvil sale del "Modo avión" (es decir, cuando este modo es desactivado; menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Modo avión"), no se solicitará el PIN de la tarjeta SIM al usuario (tal y como ocurría en versiones previas de Android), al activarse de nuevo los servicios de telefonía móvil. El valor del PIN ha sido almacenado en memoria para disponer de nuevo de acceso a la tarjeta SIM:

5.4.2 CÓDIGO DE ACCESO AL DISPOSITIVO MÓVIL

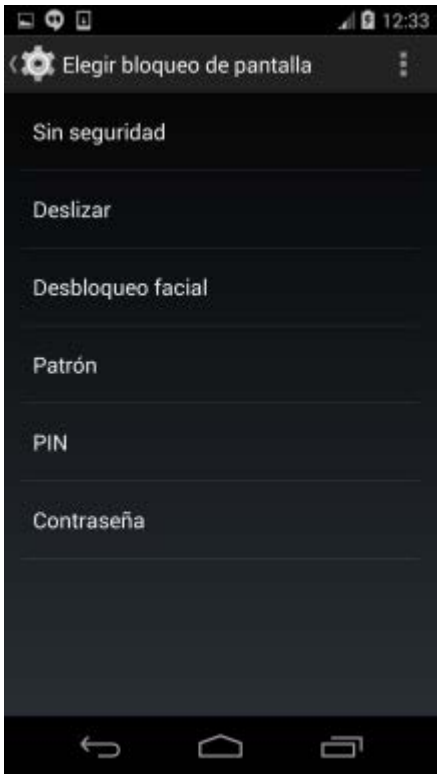
277. El código de acceso (PIN, contraseña, patrón de acceso, etc) del dispositivo móvil bloquea el acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones móviles (o apps).

278. Una vez el dispositivo móvil está bloqueado, únicamente se permite la realización de llamadas de emergencia (112) sin el código de acceso del terminal. Para ello es necesario marcar el número de teléfono de emergencias tras pulsar el texto "Llamada de emergencia" (situado en la parte inferior de la pantalla).

279. Sin embargo, si únicamente se establece el código de acceso en el dispositivo móvil y no un PIN en la tarjeta SIM (ver apartado "5.4.1. PIN de la tarjeta SIM"), aún es posible para un potencial atacante acceder físicamente al terminal, extraer la tarjeta SIM y hacer uso de la misma en otro terminal, incluidos sus servicios y capacidades de telefonía móvil asociados.

280. Por defecto, los dispositivos móviles basados en Android no disponen de un código de acceso para evitar accesos no autorizados al terminal.

281. Se recomienda por tanto establecer un código de acceso al dispositivo móvil a través del menú "Ajustes [Personal] - Seguridad - Bloqueo de pantalla":

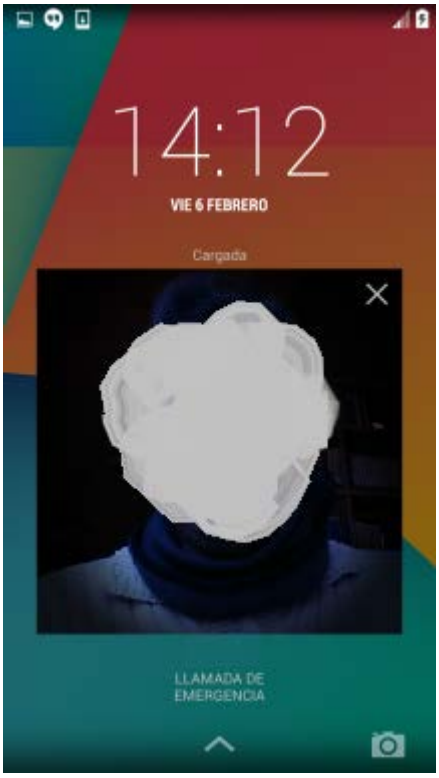


282. Android permite establecer múltiples tipos de códigos de acceso:

- "Sin seguridad" (o "Ninguno"): deshabilita por completo la pantalla de desbloqueo.

- "Deslizar": no establece ningún código de acceso, siendo necesario únicamente deslizar el icono con un candado cerrado de la pantalla de desbloqueo hacia la circunferencia asociada a un icono con un candado abierto.

- "Desbloqueo facial" (*Face Unlock*, disponible desde Android 4.0, *Ice Cream Sandwitch* [Ref.- 83]): permite emplear biometría, y en concreto, los rasgos de la cara del usuario para desbloquear el dispositivo móvil mediante reconocimiento facial, tomando previamente, durante el proceso de configuración, una imagen de la cara del usuario.



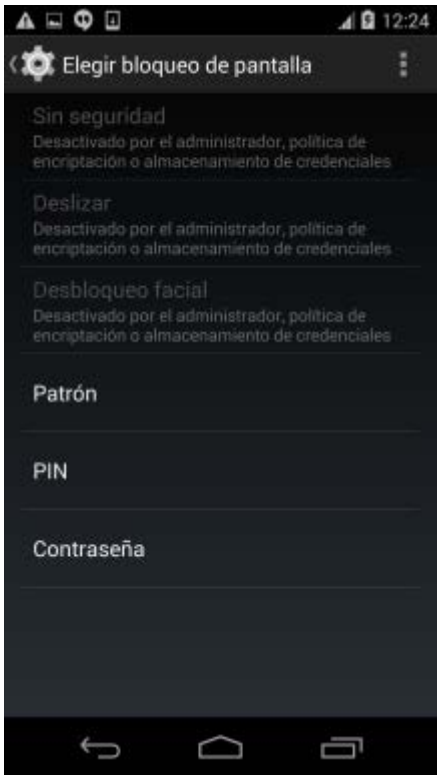
Al emplearse el "Desbloqueo facial", en el caso en que no se pueda reconocer al usuario, debe fijarse un método de desbloqueo alternativo, pudiendo elegir entre "Patrón" o "PIN".

- "Patrón": permite establecer un patrón de desbloqueo de pantalla, a través del cual es posible definir un patrón de movimiento (en una matriz de 3x3 puntos ubicada en la pantalla del dispositivo móvil) para proceder a desbloquear el dispositivo móvil.

- "PIN": permite establecer un PIN o código numérico tradicional, compuesto por al menos cuatro dígitos (0-9), no desvelándose en la pantalla de desbloqueo la longitud del mismo.

- "Contraseña": permite establecer una contraseña alfanumérica, compuesta por al menos cuatro caracteres alfanuméricos (incluyendo letras minúsculas, mayúsculas, dígitos y símbolos de puntuación), y por tanto, opción más segura y recomendada.

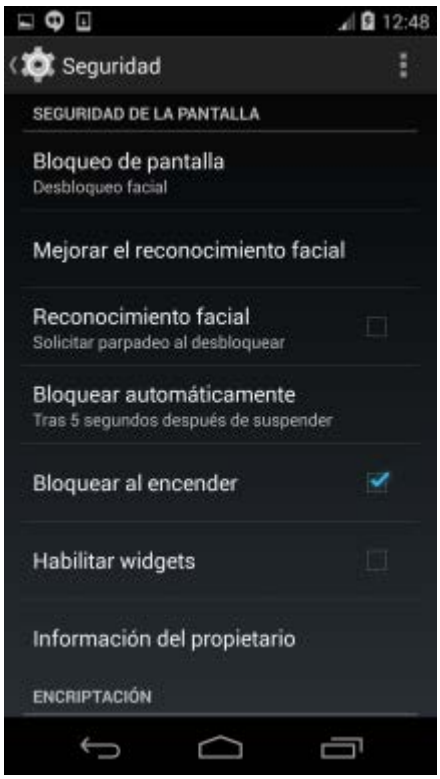
283. En el caso en el que se hayan activado otras capacidades de seguridad del dispositivo móvil, como por ejemplo el almacenamiento de credenciales (ver apartado "5.7. Gestión de certificados digitales y credenciales en Android") o el cifrado completo del dispositivo móvil (ver apartado "5.6. Cifrado de datos en Android"), algunas de las opciones más sencillas e inseguras para el desbloqueo del terminal desde la pantalla de acceso no estarán disponibles:

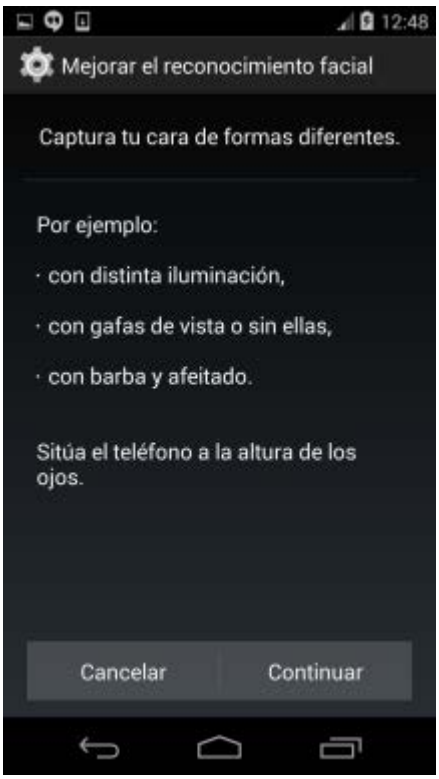


284. Las opciones "Sin seguridad" o "Deslizar" están completamente desaconsejadas desde el punto de vista de seguridad, ya que exponen el dispositivo móvil a accesos no autorizados si un potencial atacante obtiene acceso físico al mismo, incluso temporalmente.

285. Asimismo, la utilización de la opción de "Desbloqueo facial" está desaconsejada desde el punto de vista de seguridad, ya que es posible desbloquear el dispositivo móvil empleando una fotografía o imagen del usuario.

286. Por este motivo, versiones posteriores de Android (en concreto, disponible desde Android 4.1, *Jelly Bean*), han añadido opciones como por ejemplo "Reconocimiento facial (Solicitar parpadeo al desbloquear)", para verificar que no se está empleando una fotografía estática. Sin embargo, esta verificación también puede ser potencialmente evitada empleando imágenes animadas:

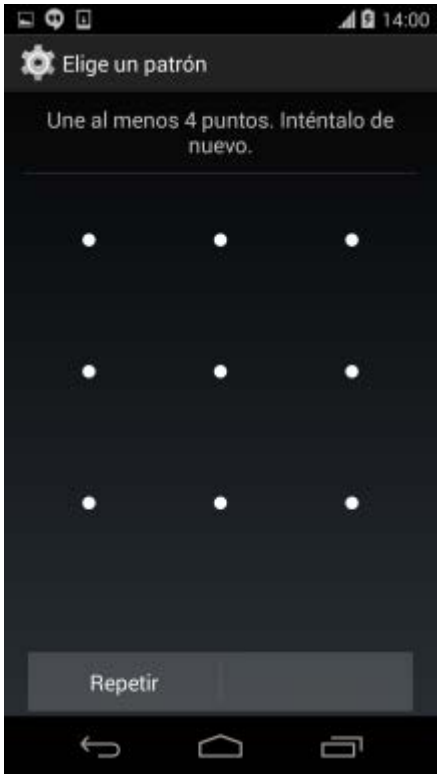


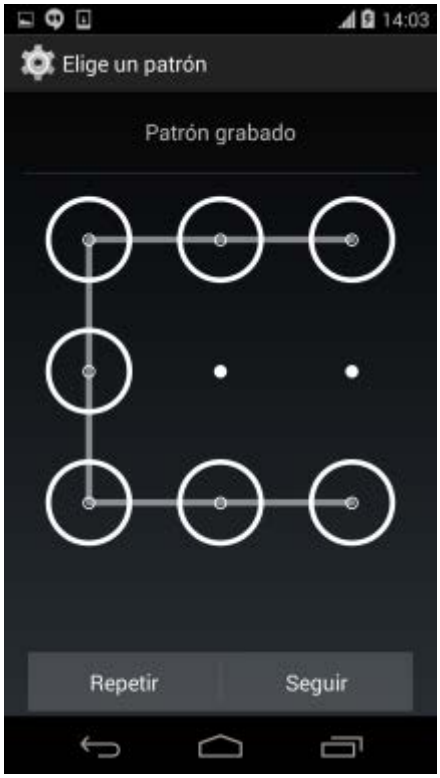


287. Adicionalmente, Android 4.1 también introdujo la opción "Mejorar el reconocimiento facial", que permite capturar la cara del usuario en distintos escenarios (distintas iluminaciones, con o sin gafas, afeitado y sin afeitar, etc), con el objetivo de obtener los rasgos principales de la misma.

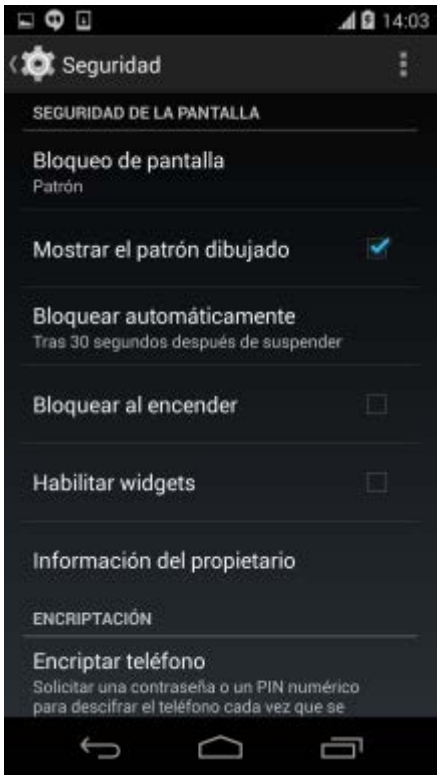
288. Al seleccionar la opción "Patrón", Android proporciona la ayuda necesaria para que el usuario aprenda a crear un patrón de desbloqueo, siendo necesario que el patrón incluya al menos cuatro puntos de los nueve (matriz de 3 x 3, por defecto) en los que se divide la pantalla del dispositivo móvil.

289. El número máximo de puntos posibles en el patrón de desbloqueo es de nueve, ya que no es posible repetir la selección de un mismo punto. Por tanto, se recomienda emplear patrones de desbloqueo complejos, que hagan uso de un mayor número de puntos, como por ejemplo, de 6 a 9 (y en ningún caso del número mínimo de tan sólo 4 puntos).



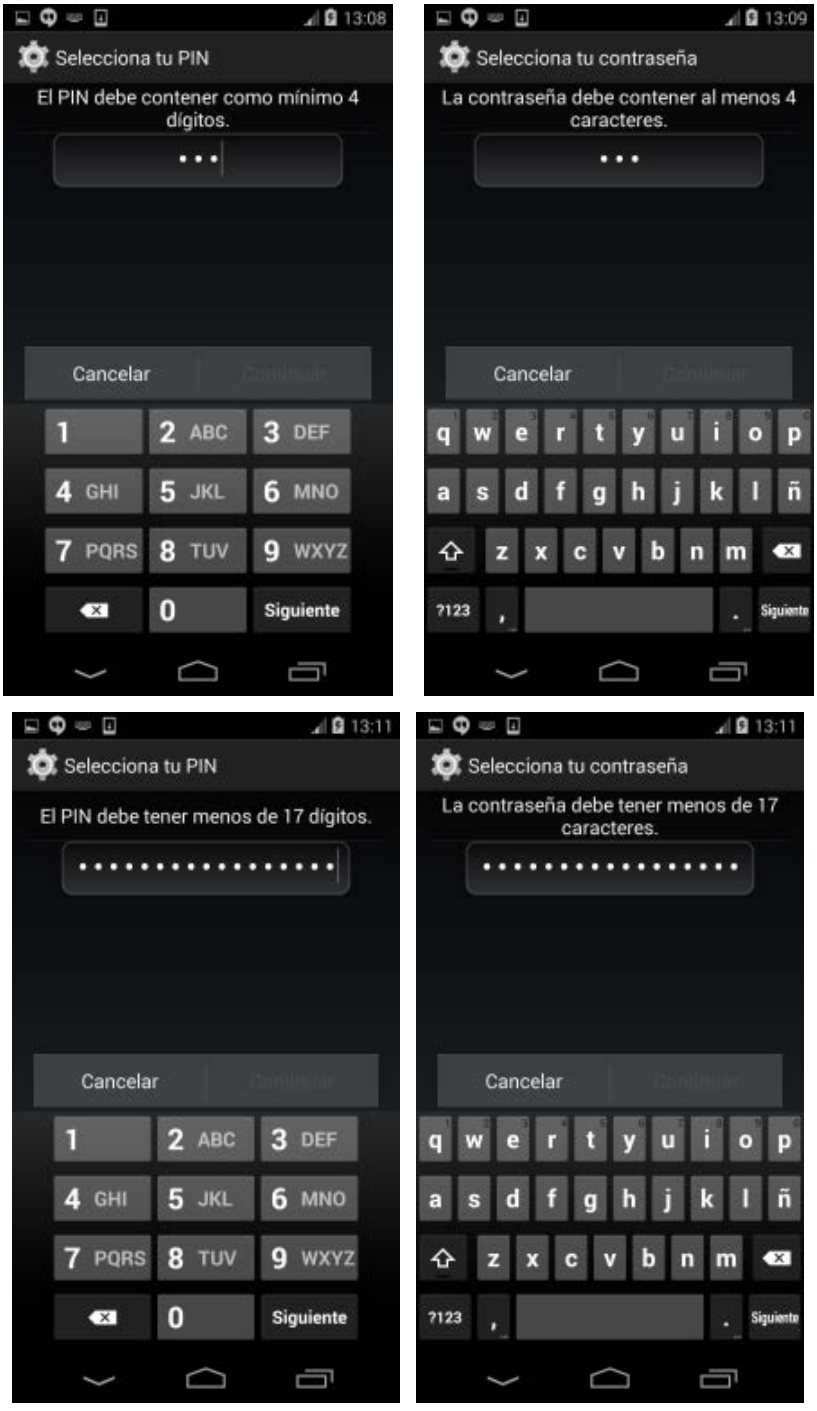


290. En caso de seleccionar un patrón de desbloqueo, es posible definir si el patrón es o no visible durante el proceso de desbloqueo del dispositivo móvil mediante la opción "Mostrar el patrón dibujado" (habilitada por defecto). En cualquier caso, Android proporcionará una respuesta táctil durante la introducción del patrón mediante una pequeña vibración al seleccionar cada punto de la matriz (opción que no puede ser deshabilitada en Android 4.x):



291. Desde el punto de vista de seguridad se recomienda no habilitar el uso de un patrón visible (que dibujaría las líneas de unión entre los puntos que conforman el patrón), para evitar que alguien con acceso visual al dispositivo móvil durante el proceso de desbloqueo pueda obtener el patrón empleado.

292. El tamaño mínimo tanto del PIN como de la contraseña alfanumérica en Android es de 4 dígitos o caracteres. El tamaño máximo de ambos es de 16 dígitos o caracteres respectivamente:

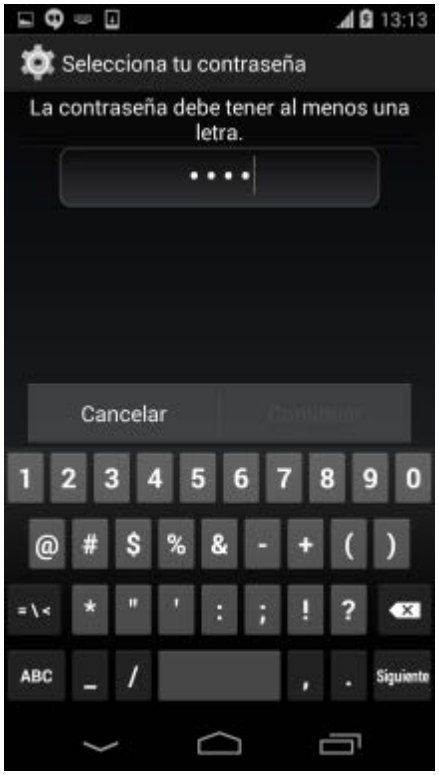


293. Android no realiza ninguna verificación de seguridad sobre el valor del PIN o contraseña elegidos, permitiendo el uso de secuencias simples de dígitos o caracteres, como por

ejemplo secuencias conocidas, que se repiten o que siguen un patrón entre sus dígitos o letras, como 1111, 1234, aaaa, etc.

294. Adicionalmente, en el caso de emplear una contraseña alfanumérica (opción recomendada), por defecto Android no aplica restricciones complejas sobre su contenido, no obligando a que contenga valores en diferentes categorías de las cuatro siguientes: letras minúsculas, letras mayúsculas, números (o dígitos) y símbolos de puntuación.

295. La única restricción de las contraseñas es que contengan al menos una letra, para diferenciarlas de los PIN, basados únicamente en dígitos:



296. Al emplear una contraseña de acceso, Android permite definir si se muestran o no los valores de los caracteres introducidos (únicamente el último dígito o carácter pulsado) mientras se escribe, a través de la opción "[Contraseñas] Mostrar las contraseñas" (habilitada por defecto) y disponible desde el menú "Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]".

297. Desde el punto de vista de seguridad se recomienda no habilitar el uso de contraseñas visibles, para evitar que alguien con acceso visual a la pantalla del dispositivo móvil durante el proceso de desbloqueo pueda obtener la contraseña empleada.

298. En el caso de utilizar un PIN, esta configuración sólo aplicaría durante el proceso de configuración y selección del PIN, ya que la pantalla de desbloqueo siempre muestra (mediante la iluminación de la tecla empleada) el dígito pulsado por el usuario. Por este motivo, entre otros, se debe prestar especial atención a quién dispone de acceso visual a la pantalla durante el proceso de desbloqueo.

299. Pese a la debilidad asociada al uso de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, Android implementa un mecanismo que hace que sólo sea posible introducir cinco códigos de acceso (PIN, contraseñas o patrones) incorrectos cada periodo de (al menos) 30 segundos, independientemente de si el valor introducido es siempre el mismo:

300. Tras introducir cinco veces un código de acceso incorrecto el dispositivo móvil bloquea la posibilidad de acceso durante 30 segundos, notificando al usuario este hecho y mostrando

un contador de cuenta atrás que indica los segundos pendientes hasta poder volver a intentar acceder al dispositivo (19 segundos en el ejemplo de la imagen superior).

301. Este mecanismo sólo permite la realización de ataques de adivinación o fuerza bruta del código de acceso con un máximo de 600 intentos por hora. Este cálculo considera el caso ideal para el atacante, con un máximo de cinco intentos cada 30 segundos, despreciando el tiempo empleado para realizar los propios intentos de acceso.

302. Para proceder a modificar el código de acceso al dispositivo móvil, en caso de disponer de un valor ya fijado, es necesario introducir el código de acceso (PIN, contraseña o patrón) actual.

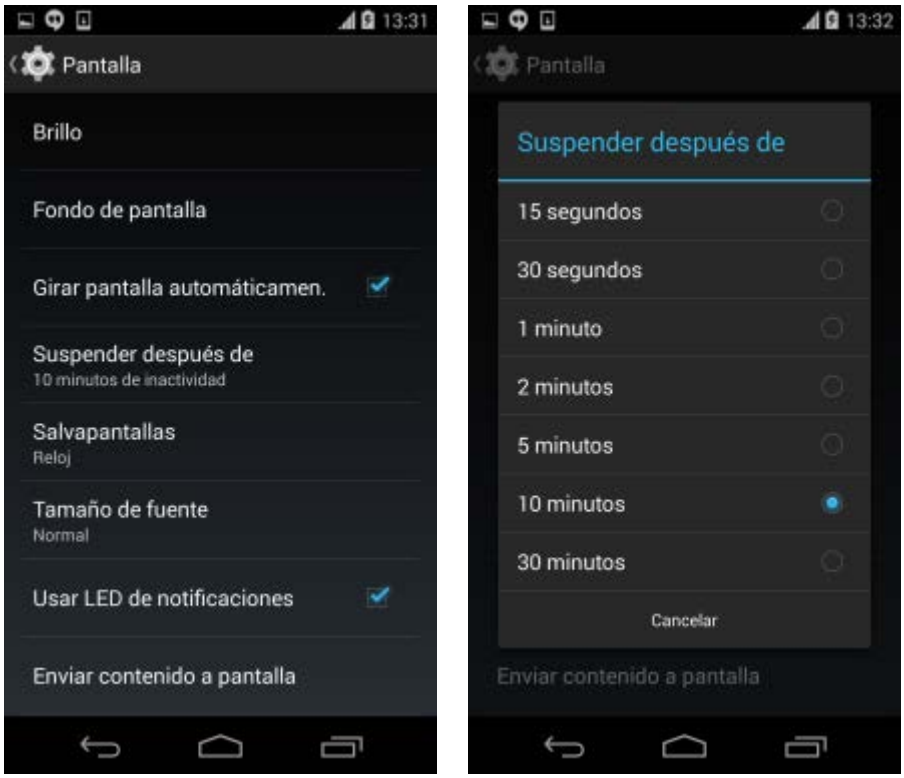
5.4.3 ACTIVACIÓN DE LA PANTALLA DE DESBLOQUEO

303. Una vez ha sido establecido el código de acceso, el dispositivo móvil solicitará al usuario éste para proceder a desbloquear el acceso al terminal cada vez que esté bloqueado, como por ejemplo al encender el terminal o tras un tiempo de inactividad.

304. La configuración que permite determinar cuando la pantalla del dispositivo móvil será bloqueada tras un periodo de inactividad depende de dos factores o parámetros de configuración (analizados en detalle a continuación). Por un lado, depende de cuando se suspenderá la pantalla tras un tiempo de inactividad y, por otro, de cuando se bloqueará la pantalla después de haber sido suspendida.

305. Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad, mediante el ajuste de la configuración de ambos parámetros, por ejemplo a 1 minuto. El rango razonable, buscando el equilibrio entre seguridad y usabilidad, debería estar entre 1 y 2 minutos, pero debe ser definido por la política de seguridad de la organización propietaria del terminal.

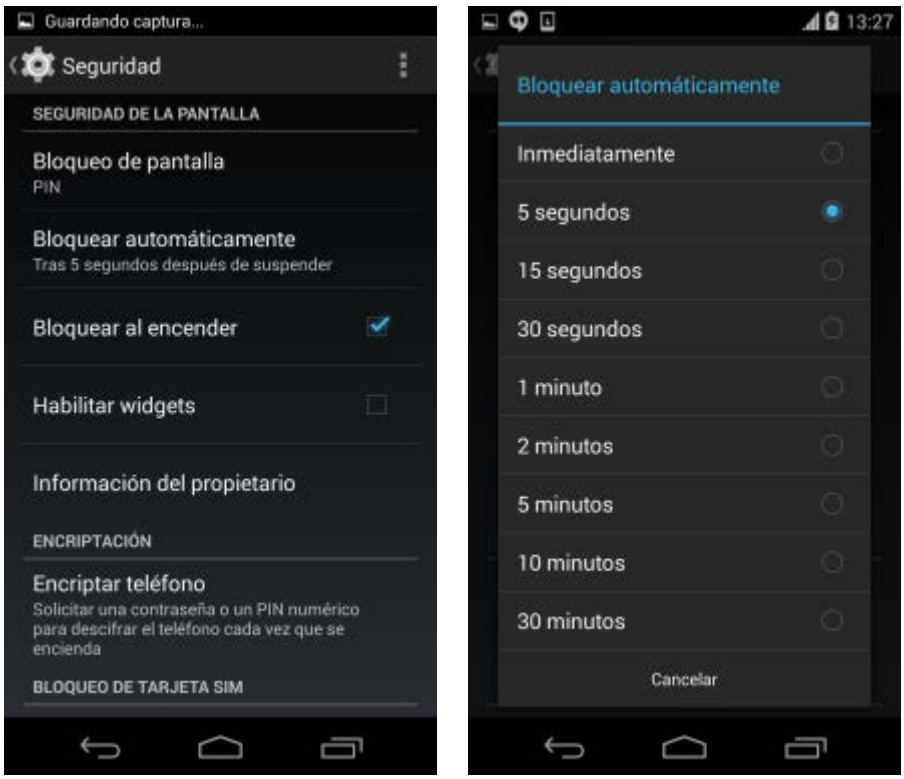
306. Por un lado, el tiempo de bloqueo de la pantalla por inactividad se establece a través del menú "Ajustes [Dispositivo] - Pantalla - Suspender después de":



307. Android proporciona un rango de valores temporales para suspender la pantalla de entre 15 segundos y 30 minutos, siendo el valor por defecto de 2 minutos (si no se ha configurado una cuenta de usuario de Google, y de 30 segundos si se ha vinculado una cuenta de usuario de Google con el dispositivo móvil).

308. Como se puede ver, Android no dispone de una opción que permita que la pantalla permanezca indefinidamente activa y que no se suspenda en ningún momento, independientemente del periodo de inactividad, con el objetivo de gestionar el consumo de batería del dispositivo, siendo el periodo máximo de 30 minutos.

309. Por otro lado, el tiempo de bloqueo de la pantalla una vez suspendida por inactividad se establece a través del menú "Ajustes [Personal] - Seguridad [Seguridad de la Pantalla] - Bloquear automáticamente":



310. Android proporciona un rango de valores temporales para bloquear la pantalla tras suspender el dispositivo móvil de entre 5 segundos y 30 minutos, con la posibilidad de bloquear la pantalla inmediatamente (opción más segura), siendo el valor por defecto (una vez fijado un código de acceso) de 5 segundos.

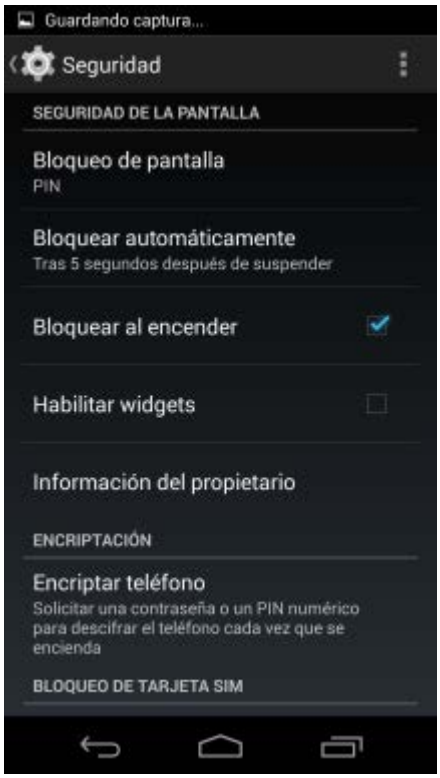
311. Como se puede ver, Android no dispone de una opción que permita que la pantalla quede sin bloquear indefinidamente tras un periodo de inactividad, opción desaconsejada desde el punto de vista de seguridad en el caso de que existiera, siendo el periodo máximo de 30 minutos.

312. En resumen, se recomienda encontrar el equilibrio entre ambos parámetros de configuración para que se lleve a cabo la activación de la pantalla de desbloqueo tras un periodo de inactividad, por ejemplo, fijando el valor de "Suspender después de" a 1 minuto y el de "Bloquear automáticamente" a 30 segundos, lo que implicaría que pasarían menos de 2 minutos antes del bloqueo.

313. Adicionalmente, la configuración asociada al bloqueo de la pantalla del dispositivo móvil tras un periodo de inactividad se complementa con el siguiente parámetro de

configuración, que determina si la pantalla debe ser bloqueada cuando la pantalla del dispositivo móvil es apagada manualmente por el usuario mediante el botón de encendido (pero únicamente la pantalla, sin apagar por completo el dispositivo móvil).

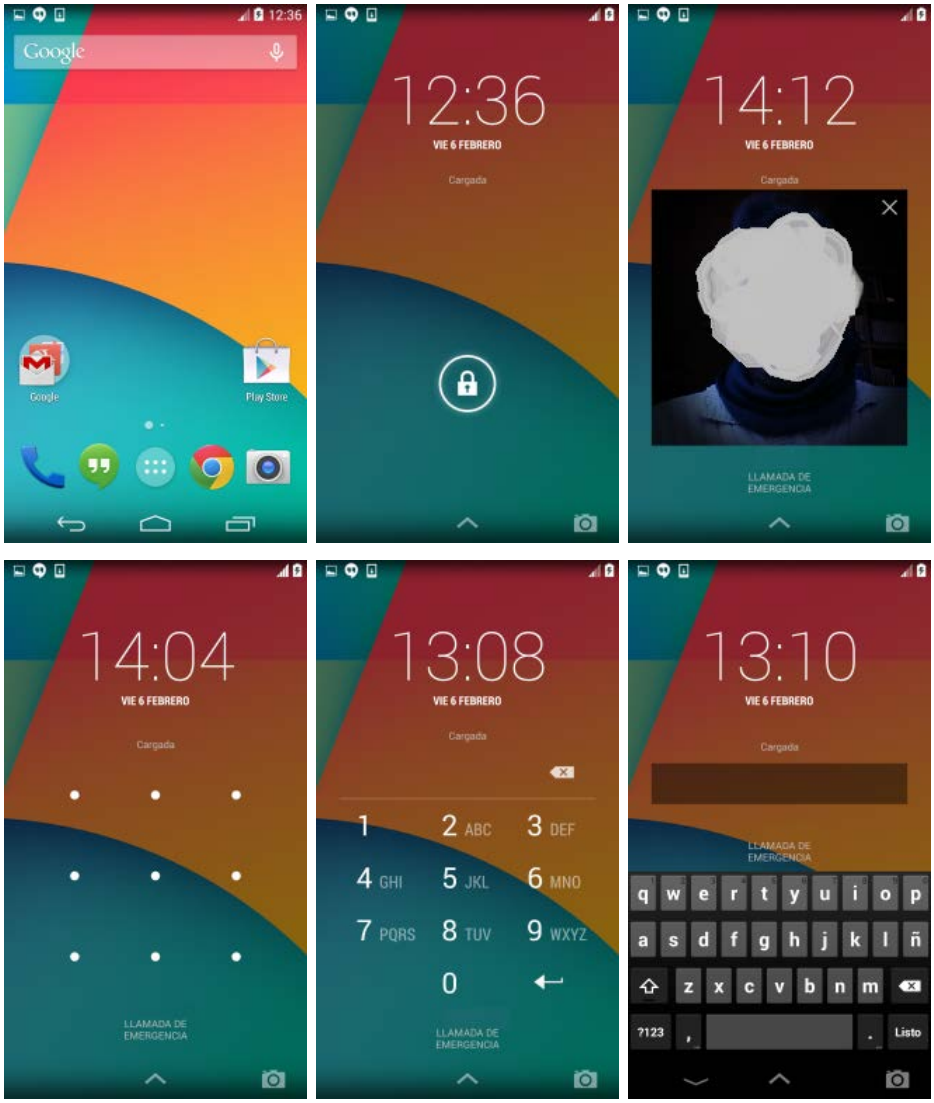
314. La opción "Bloquear al encender", disponible desde el menú "Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]", cuando está activa, implica que el evento de apagar la pantalla manualmente por parte del usuario fuerza un bloqueo de la pantalla. Al encenderla de nuevo será necesario siempre introducir el código de acceso para desbloquearla:



315. Sin embargo, si esta opción no es activada, el evento de apagar la pantalla manualmente por parte del usuario es equivalente a que el dispositivo móvil se suspenda tras un periodo de inactividad. Dependiendo del valor del parámetro "Bloquear automáticamente" (descrito previamente) se bloqueará la pantalla tras el tiempo especificado.

5.4.4 PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS

316. En primer lugar, como se puede apreciar en las siguientes imágenes, la pantalla de desbloqueo de Android permite diferenciar visualmente entre las diferentes configuraciones de desbloqueo del terminal (ninguno, deslizar, desbloqueo facial, patrón, PIN, o contraseña), lo que puede facilitar a un potencial atacante una primera aproximación al nivel de seguridad existente en el dispositivo móvil:



317. La pantalla de desbloqueo del dispositivo móvil (*lock screen*) en Android permite, sin necesidad de introducir el código de acceso y, por tanto, sin necesidad de desbloquear el terminal, junto a la hora y la fecha, la previsualización del nombre del operador de telecomunicaciones (en la parte inferior central - eliminado en las imagenes previas) y de la barra superior de estado, que incluye los iconos de conectividad y de notificaciones.

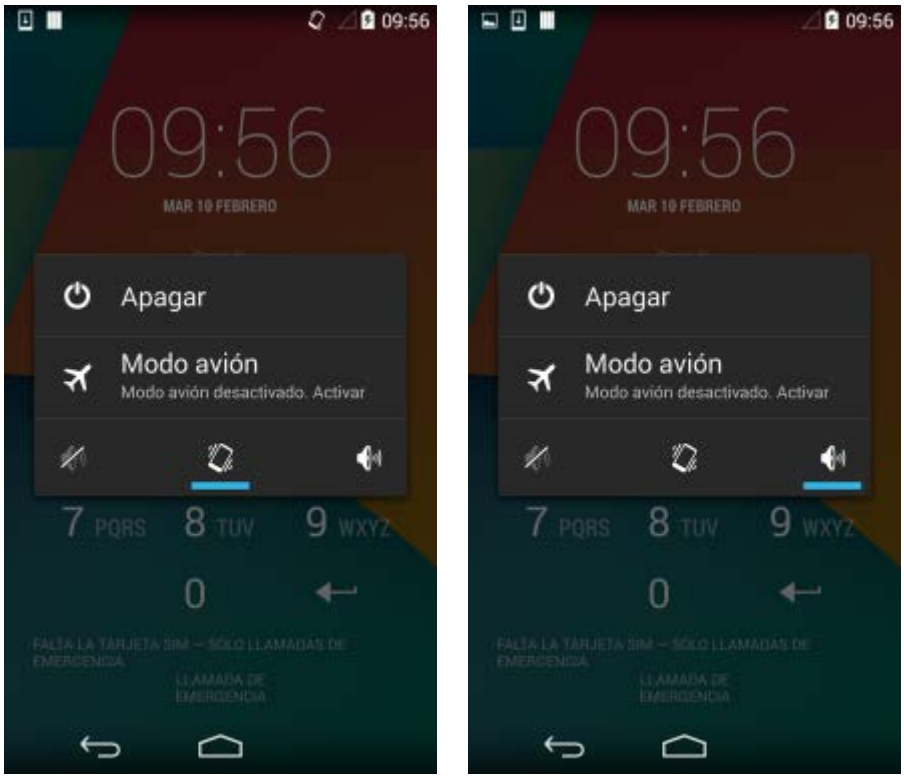
318. La pantalla de desbloqueo de Android 4.x ha minimizado la posibilidad de desvelar información potencialmente confidencial y sensible a un potencial atacante. Por ejemplo, en el caso de recibirse un mensaje SMS, se indica mediante un aviso sonoro y una vibración (por defecto), pero no se muestra el contenido del mismo ni en la pantalla de desbloqueo ni en la barra superior de estado.

319. Sin embargo, la información desvelada puede extenderse mediante la utilización de *widgets* en la pantalla de desbloqueo (ver apartado "5.4.6. Pantalla de desbloqueo: Widgets").

5.4.5 PANTALLA DE DESBLOQUEO: APAGAR EL DISPOSITIVO MÓVIL

320. Desde la pantalla de desbloqueo de Android, y sin conocer el código de acceso pero disponiendo de acceso físico temporal al dispositivo móvil, es posible mantener pulsado el botón de encendido y apagado para proceder a apagar el terminal.

321. Antes de que éste sea apagado, se muestra un menú que permite tanto apagar el dispositivo móvil, como gestionar el sonido, indicando si está en silencio, en modo vibración, o con el volumen activo:



322. Adicionalmente, este menú permite activar el modo avión (o modo vuelo, botón "Modo avión"), lo que supone un riesgo desde el punto de vista de seguridad, ya que si una persona no autorizada obtiene acceso físico al dispositivo móvil y activa el modo avión, no será posible disponer de conectividad de datos desde el dispositivo móvil para poder hacer uso de las capacidades remotas de gestión del mismo (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android"), por ejemplo, en escenarios donde se ha perdido el dispositivo móvil, o éste ha sido robado[38].

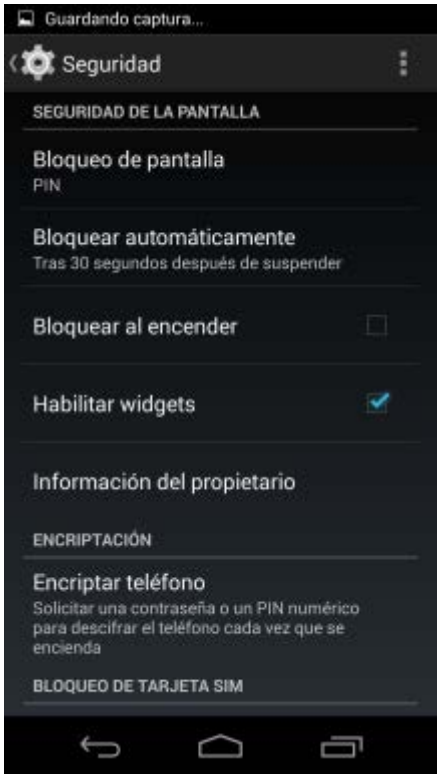
323. Desafortunadamente, Android no proporciona ningún ajuste de configuración que permita deshabilitar el botón "Modo avión" en el menú disponible al apagar el terminal.

5.4.6 PANTALLA DE DESBLOQUEO: WIDGETS

324. Android, desde la versión 4.2[39], permite añadir *widgets* (o complementos) que permiten mostrar información y contenidos en la pantalla de desbloqueo, especialmente cuando ésta se encuentra bloqueada.

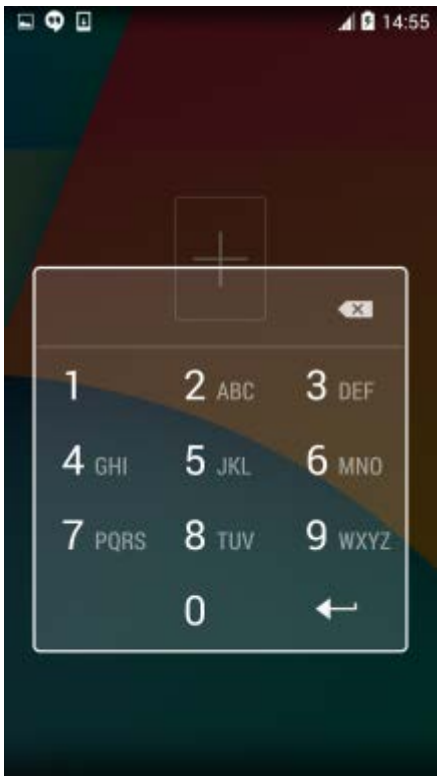
325. Por defecto, estas capacidades están deshabilitadas, pero pueden ser habilitadas a través del menú "Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]" y la opción "Habilitar widgets":

[38] En este escenario el dispositivo móvil está encendido, y por ejemplo, su memoria ya ha sido descifrada.
[39] http://developer.android.com/about/versions/android-4.2.html#Lockscreen



326. Los *widgets* representan normalmente versiones reducidas de ciertas apps, y permiten mostrar la información más relevante de las mismas, como por ejemplo, mensajes de e-mail, citas de calendario o información meteorológica [Ref.- 161].

327. Por defecto en la pantalla de desbloqueo se muestra únicamente el *widget* asociado al reloj digital, pero es posible añadir nuevos *widgets* (una vez activada la opción descrita previamente) deslizando la pantalla de desbloqueo de izquierda a derecha:



328. Mediante el símbolo "+" y tras introducir el código de acceso, se obtiene la lista de *widgets* disponibles (en función de las apps existentes por defecto e instaladas), pudiéndose añadir hasta cinco *widgets* a la pantalla de desbloqueo:

329. Los *widgets* pueden ser eliminados de la pantalla de desbloqueo, tras ocultar el teclado empleado para introducir el código de acceso (deslizándolo hacia la parte inferior de la pantalla), mediante una pulsación prolongada sobre el *widget*, y arrastrándolo hacía el texto "X Eliminar" existente en la parte superior de la pantalla.

330. Para eliminar un *widget* no es necesario introducir el código de acceso.

331. Una vez se ha desbloqueado el dispositivo móvil, desde la pantalla principal o de inicio, es posible organizar los diferentes iconos y elementos mediante una pulsación larga sobre la misma. Asimismo, esta pulsación permite disponer de acceso al icono "Widgets" (en la parte inferior central) para su selección:

332. Desde el punto de vista de seguridad, en el caso de querer hacer uso de *widgets*, se debe ser muy cuidadoso a la hora de seleccionar qué *widgets* se incluirán en la pantalla de desbloqueo, y qué tipo de información, potencialmente sensible, es mostrada por estos.

333. Estas capacidades complementan al resto de información disponible por defecto en la pantalla de desbloqueo (ver apartado "5.4.4. Pantalla de desbloqueo: Previsualización de datos"):

5.4.7 PANTALLA DE DESBLOQUEO: CÁMARA

334. Android, desde la versión 4.0 (*Ice Cream Sandwich*), permite hacer uso de la cámara (para hacer fotografías o grabar vídeos) desde la pantalla de desbloqueo sin necesidad de desbloquearla mediante el código de acceso [Ref.- 161].

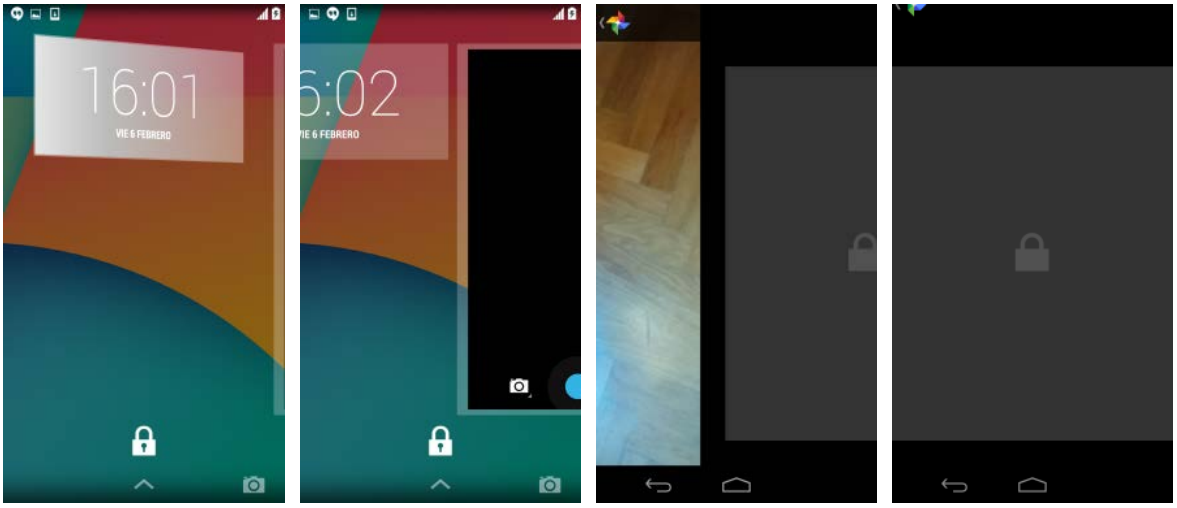
335. El acceso a la cámara desde la pantalla de desbloqueo no está disponible en las tabletas basadas en Android, únicamente en los *smartphones*.

336. El icono de acceso directo a la cámara desde la pantalla de desbloqueo está disponible en la parte inferior derecha, mediante un icono de un cámara. Si se desplaza dicho icono (o la propia pantalla de desbloqueo) hacia la izquierda, se accede a la cámara, disponiendo de acceso completo a la misma y a todas sus opciones de configuración:

337. Esta funcionalidad tiene implicaciones relevantes desde el punto de vista de seguridad, ya que alguien sin autorización que obtenga acceso físico temporalmente al dispositivo móvil puede hacer fotografías o vídeos, como si estos hubieran sido realizados por el usuario del terminal.

338. La cámara no puede ser eliminada de la pantalla de bloqueo, ya que Android no dispone de ningún ajuste de configuración con este propósito.

339. Debe tenerse en cuenta que desde la pantalla de bloqueo, respecto a la funcionalidad de la cámara, y sin conocer el código de acceso, sólo se dispone de acceso a las fotografías y vídeos que han sido realizados en la sesión actual (desplazando la pantalla de la cámara hacia la izquierda), no pudiendo accederse al resto de fotografías y vídeos:

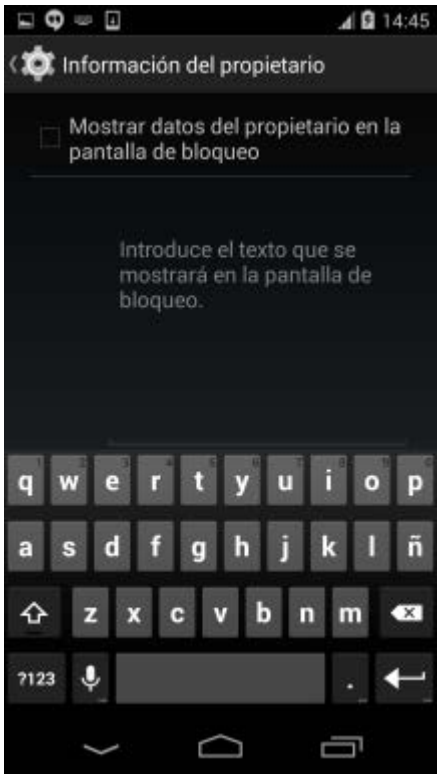


5.4.8 PANTALLA DE DESBLOQUEO: INFORMACIÓN DEL PROPIETARIO

340. Android permite establecer un mensaje con información del propietario en la pantalla de desbloqueo, característica que es especialmente útil cuando la pantalla se encuentra bloqueada y se extravía el dispositivo móvil.

341. Si alguien con buenas intenciones se encuentra el dispositivo móvil, puede visualizar dicho mensaje y llevar a cabo acciones en función del mismo.

342. Por defecto, el mensaje con información del propietario está deshabilitado, pero puede ser habilitado a través del menú "Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]" y la opción "Información del propietario":



343. Para ello debe activarse la opción "Mostrar datos del propietario en la pantalla de bloqueo" y se recomienda proporcionar un mensaje descriptivo, que sin desvelar información sensible, crítica, o que pueda ayudar a identificar detalles innecesarios del propietario,

ayude, por ejemplo, a la recuperación del dispositivo móvil. Por ejemplo, se recomienda fijar un mensaje similar al siguiente: "Si encuentra este teléfono, por favor, llame al número +34 678901234. Muchas gracias.".

5.4.9 PRECAUCIONES Y RECOMENDACIONES ADICIONALES

344. Adicionalmente a todas las opciones de configuración e implicaciones asociadas detalladas previamente, es posible establecer éstos y otros parámetros de configuración asociados al proceso de desbloqueo del dispositivo móvil a través de las políticas de seguridad de Google Apps (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android").

345. Cuando se establece un código de acceso al dispositivo móvil, si el modo de depuración está habilitado (ver apartado "5.11.3. Opciones de desarrollo y depuración USB") es posible acceder al terminal mediante el interfaz USB, por ejemplo para capturar su pantalla, intercambiar datos, gestionar sus ficheros, instalar apps y leer datos del registro de actividades, sin necesidad de desbloquear el dispositivo móvil. Un atacante, mediante acceso físico al terminal, podría potencialmente realizar múltiples tareas de administración del dispositivo móvil sin conocer la contraseña de acceso. El impacto de las acciones que pueden ser llevadas a cabo sin conocer el código de acceso está mitigado por algunas capacidades de seguridad disponibles desde Android 4.4.2 (ver apartado "5.11.4. Relaciones de confianza a través de USB").

346. Se recomienda por tanto desde el punto de vista de seguridad deshabilitar el modo de depuración mediante el menú "Ajustes [Sistema] - Opciones de desarrollo", deshabilitando la opción "Depuración USB".

347. Una vez fijados tanto el PIN en la tarjeta SIM como el código de acceso en el dispositivo móvil, al encender el terminal, el dispositivo móvil solicitará primero el PIN de la tarjeta SIM y después el del terminal, en este orden:

348. Pese a que la obligatoriedad de introducir dos PIN (o códigos de acceso) diferentes puede suponer una molestia para el usuario, cuyos valores desde el punto de vista de seguridad se recomienda sean distintos, es necesario establecer ambos niveles de seguridad para que, tanto la tarjeta SIM y sus servicios asociados, como el dispositivo móvil y sus datos asociados, estén protegidos.

349. Adicionalmente, y con el objetivo de mejorar globalmente la seguridad de los servicios asociados al dispositivo móvil, se recomienda modificar a la mayor brevedad posible el PIN de acceso al buzón de voz proporcionado por el operador de telefonía móvil al activar este servicio. Su valor debe ser diferente al valor del código de acceso del dispositivo móvil y del PIN de la tarjeta SIM.

5.4.10 DESBLOQUEO MEDIANTE LA CUENTA DE USUARIO DE GOOGLE

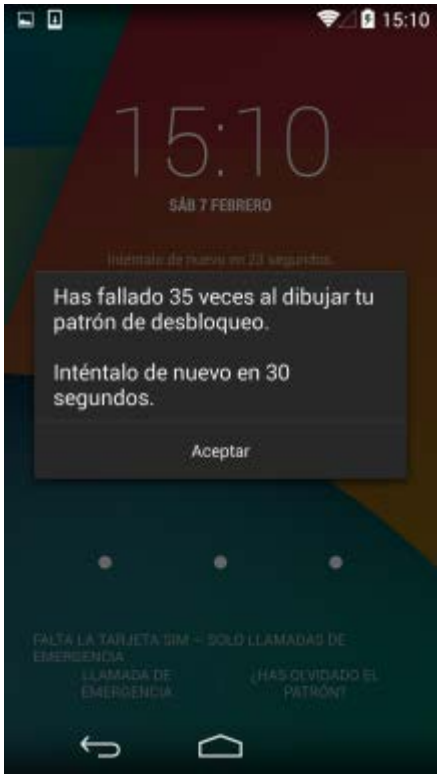
350. Si no se puede desbloquear el dispositivo móvil Android, existe la posibilidad de restablecer el código de acceso con la cuenta de usuario de Google o a través del administrador de dispositivos Android (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android").

351. Por otro lado, si el dispositivo móvil hace uso de Android 4.4 (o una versión inferior) y disponía de un patrón de acceso, al introducirlo erróneamente en diferentes ocasiones, aparecerá el mensaje "¿Has olvidado el patrón?" en la pantalla de desbloqueo [Ref.- 66].

352. Al seleccionar ese texto, y si el dispositivo móvil dispone de conexión a Internet, se solicita el nombre de usuario y la contraseña de la cuenta de usuario de Google configurada previamente en el dispositivo móvil.

353. Tras introducir las credenciales correctas, será posible establecer de nuevo las opciones de seguridad para el acceso al dispositivo móvil en la pantalla de desbloqueo y fijar un nuevo código de acceso.

354. En el caso de Android 4.4.4, esta funcionalidad ya no está disponible, al menos, si el número de intentos fallidos al introducir el patrón es igual o inferior a 45 (ejemplo inferior con 35 intentos fallidos):



5.4.11 DESBLOQUEO MEDIANTE SCREEN LOCK BYPASS

355. Mediante la instalación remota de una app desde la web de Google Play (ver apartado "5.23.1. Instalación remota de apps") es posible desbloquear un dispositivo móvil Android que se encuentra bloqueado y para el que no se conoce el código de acceso.

356. Se han identificado escenarios en los que si el terminal está bloqueado y no se dispone del código de acceso no es posible resetear el dispositivo móvil. Un usuario legítimo podría utilizar esta app para desbloquear su propio dispositivo móvil si ha olvidado el código de acceso, si desea hacer copia de seguridad de los datos contenidos en el terminal.

357. La app que permite llevar a cabo este tipo de acción se denomina "Screen Lock Bypass Pro" [Ref.- 74], actualmente de pago, y disponible públicamente en Google Play.

358. Aunque esta app tenía aplicación principalmente en las versiones 2.x de Android, dado que se introdujeron cambios en Android 4.0 que limitan que una app recién instalada pueda ser ejecutada por primera vez a través de un *broadcast intent* (obligando al usuario a ejecutarla manualmente al menos una vez), algunos dispositivos móviles no introdujeron esa modificación hasta la versión 4.0.2 de Android, permitiendo seguir empleando esta técnica y app todavía en Android 4.0 - 4.0.2 (motivo por el que es aún descrita en la presente guía).

359. Este desbloqueo remoto puede llevarse a cabo por parte de un atacante simplemente si consigue las credenciales de acceso a la cuenta principal de Google del usuario que está configurada en el dispositivo móvil Android, ya que es el único elemento necesario para instalar la app de forma remota desde la web de Google Play.

360. Una vez "Screen Lock Bypass" ha sido instalada, el evento de instalación de cualquier otra app (en las primeras versiones de esta app), o el evento de conectar el cargador USB al dispositivo móvil (o de reiniciarlo, en las últimas versiones de la app) permitirá su ejecución, y llevará a cabo el desbloqueo de la pantalla del dispositivo móvil previamente

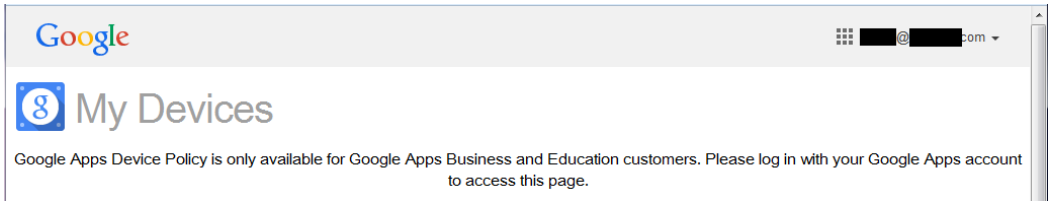
bloqueado sin conocer el código de acceso o desbloqueo. El dispositivo móvil mostrará la pantalla en la que se encontraba antes del bloqueo.

361. La instalación de las apps desde la web de Google Play se lleva a cabo de forma automática en el dispositivo móvil Android y sin ninguna intervención por parte del usuario, únicamente dejando constancia en la barra de notificaciones del dispositivo móvil (ejemplo de instalación de Screen Lock Bypass en Android 2.x):

5.4.12 RESTAURACIÓN DEL CÓDIGO DE ACCESO

362. A través de las capacidades empresariales para la gestión de dispositivos móviles basados en Android proporcionadas por Google, y específicamente a través de la plataforma Google Apps (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android"), es posible llevar a cabo de forma remota la restauración (restablecimiento o reseteo) del código de acceso y desbloqueo del dispositivo móvil desde la versión 2.2 de Android, disponiendo de la app "Google Apps Device Policy"[40] instalada [Ref.- 94].

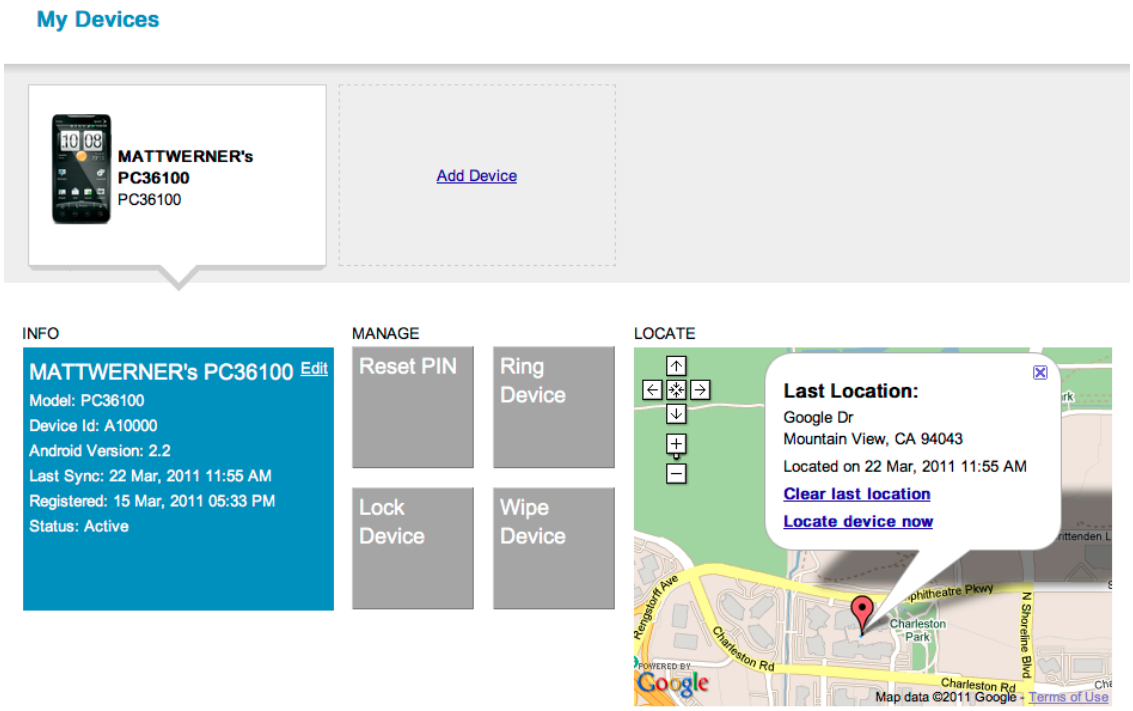
363. Esta funcionalidad sólo está disponible para los clientes de Google Apps en la categoría de Negocios (Business) o de Educación (Education):



364. El resto de usuarios que disponen de una cuenta de usuario de Google individual pueden hacer uso del "Administrador de dispositivos Android" [Ref.- 39], con funcionalidad similar pero que no dispone de las capacidades para restaurar el código de acceso del dispositivo móvil.

365. La sección "Mis dispositivos" (o "My devices"), disponible en la URL "http://www.google.com/apps/mydevices", de la página web de Google Apps dispone de una opción para llevar a cabo la restauración del código de acceso o PIN ("Reset PIN" o "Restablecer PIN") [Ref.- 61]:

[40] https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent



366. Esta funcionalidad permite a los usuarios de Google Apps la generación de un nuevo código de acceso (PIN o contraseña) para disponer de acceso al dispositivo móvil, por ejemplo, cuando el acceso al dispositivo móvil está protegido por un código de acceso y el usuario olvida dicho código de acceso.

367. El proceso se basa en la generación y utilización de un nuevo PIN que permita al usuario desbloquear el dispositivo móvil y establecer un nuevo código de acceso sin tener que eliminar los datos del dispositivo móvil (*wipe*).

5.5 MÚLTIPLES PERFILES DE USUARIO

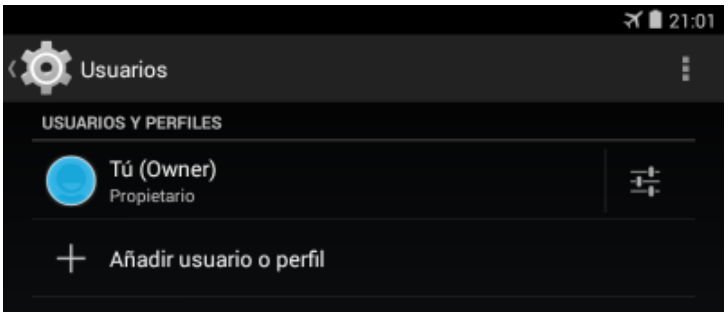
368. La versión 4.2 de Android introdujo la posibilidad de disponer de múltiples cuentas o perfiles de usuario, pudiendo cada usuario personalizar la pantalla de desbloqueo, el fondo de pantalla del escritorio, los complementos (*widgets*), las aplicaciones móviles (apps) y carpetas, ficheros, cuentas, y ajustes de configuración. Cada usuario dispone de un entorno separado, incluyendo almacenamiento separado en la tarjeta de almacenamiento externa (o tarjeta SD, en caso de existir), mediante emulación.

369. Estas capacidades están únicamente disponibles para tabletas (dispositivos móviles que se supone son compartidos más frecuentemente), y no para *smartphones*, y permiten compartir una tableta basada en Android entre distintos usuarios, teniendo cada uno de ellos acceso a su espacio dedicado de usuario, es decir, a su información desde la pantalla de desbloqueo.

370. La versión 4.3 introdujo la capacidad de poder restringir estos perfiles [Ref.- 134], pudiendo gestionar (habilitar o deshabilitar) el acceso a apps, servicios, ajustes de configuración, funcionalidades (como los servicios de localización o la posibilidad de realizar compras dentro de las apps, *in-app purchases*) y contenidos para cada usuario [Ref.- 135]. Esta nueva funcionalidad permite la aplicación de controles parentales, restringiendo el acceso a ciertas funcionalidades a los menores de edad, o la utilización de tabletas Android en entornos específicos, como por ejemplo museos o tiendas.

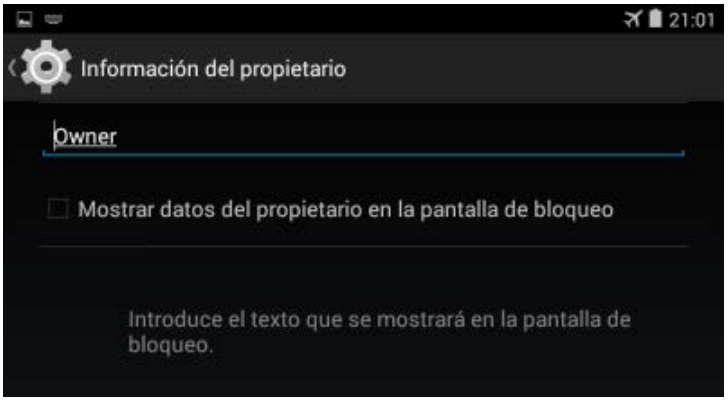
371. Las capacidades multiusuario en *smartphones* basados en Android 4.x sólo están disponibles si se lleva a cabo el proceso de *rooting* del dispositivo móvil, pero no oficialmente. Esta limitación se ha establecido en Android definiendo que el número máximo de usuarios en los *smartphones* es igual a uno.

372. La gestión de usuarios y perfiles restringidos está disponible a través del menú "Ajustes [Dispositivo] - Usuarios". La pantalla de "Usuarios y Perfiles" muestra por defecto el usuario actual, también identificado como administrador o propietario del dispositivo ("Owner"):



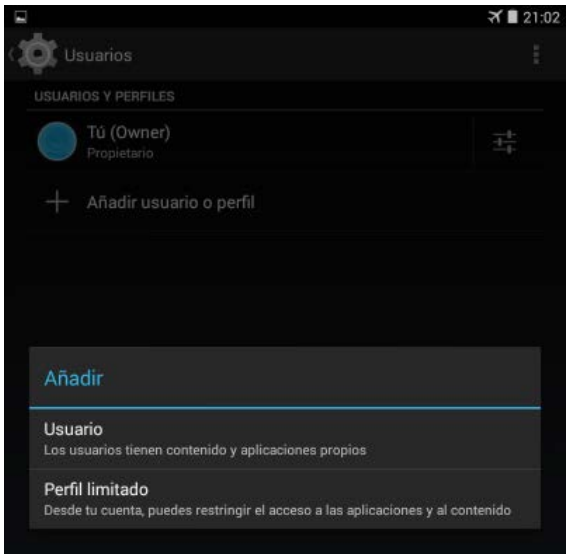
373. El usuario que inicializa el dispositivo móvil en el momento de su instalación y configuración inicial es considerado el usuario propietario (o usuario principal) del dispositivo, y dispone de mayores privilegios (desde el punto de vista de las capacidades multiusuario de Android).

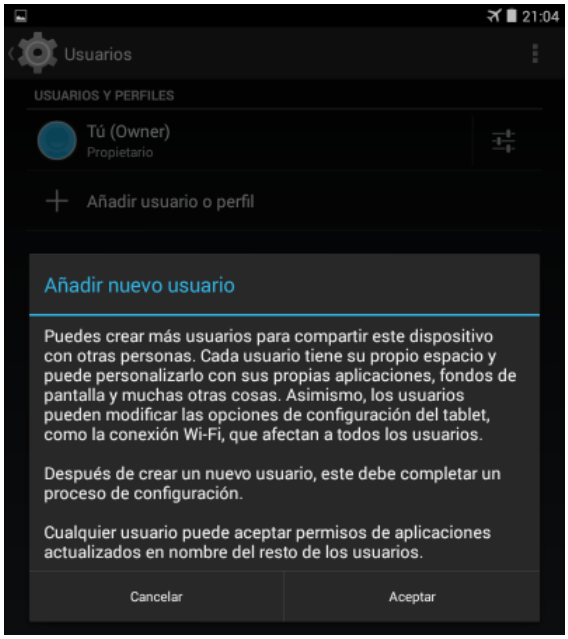
374. Los ajustes específicos de cada perfil o usuario, disponibles a la derecha del mismo, permiten establecer el nombre del usuario, y definir si se mostrarán datos del usuario en la pantalla de desbloqueo, pudiendo definir el texto a mostrar:



375. Esta información podría revelar datos relacionados con los usuarios existentes en los dispositivos móviles con las capacidades multiusuario habilitadas, añadiéndose a los datos descritos en el apartado "5.4.4. Pantalla de desbloqueo: Previsualización de datos" o emplearse para mostrar información en la pantalla de desbloqueo intencionadamente (ver apartado "5.4.8. Pantalla de desbloqueo: Información del propietario").

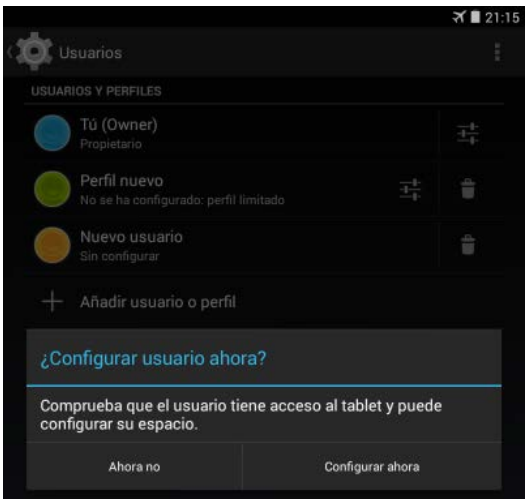
376. A la hora de añadir nuevos usuarios, mediante la opción "Añadir usuario o perfil", estos pueden asociarse a dos tipos de perfiles: usuario (regular o estándar) y perfil limitado (o usuario restringido). Un usuario (regular o estándar) dispone de sus propias apps y contenidos. Un usuario (restringido) con un perfil limitado, dispone de acceso a un conjunto limitado de apps y contenidos pertenecientes a la cuenta del usuario propietario del dispositivo móvil:





377. Los usuarios estándar disponen de sus propias apps, contenidos, y de la posibilidad de modificar ajustes de configuración generales, como por ejemplo los asociados a la red Wi-Fi. Asimismo, cualquier usuario puede aceptar nuevos permisos en el proceso de actualización de apps (ver imagen superior derecha), afectando globalmente desde el punto de vista de seguridad al dispositivo móvil y al resto de usuarios.

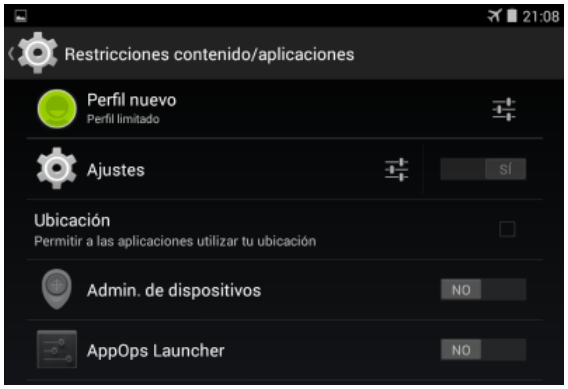
378. Tras añadir un nuevo usuario, se sugiere llevar a cabo el proceso de configuración inicial de su espacio de usuario, tarea que puede ser pospuesta para más tarde o llevada a cabo en este momento:



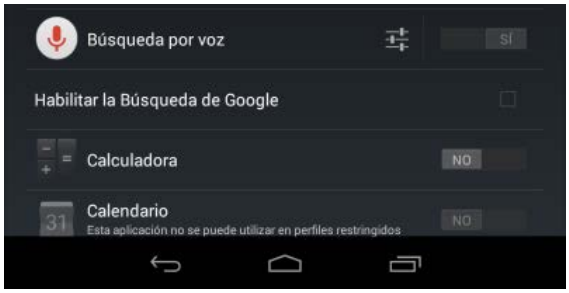
379. El proceso de configuración de un nuevo usuario (desde la pantalla de desbloqueo) conlleva un proceso similar al de configuración inicial del dispositivo móvil, pero en los

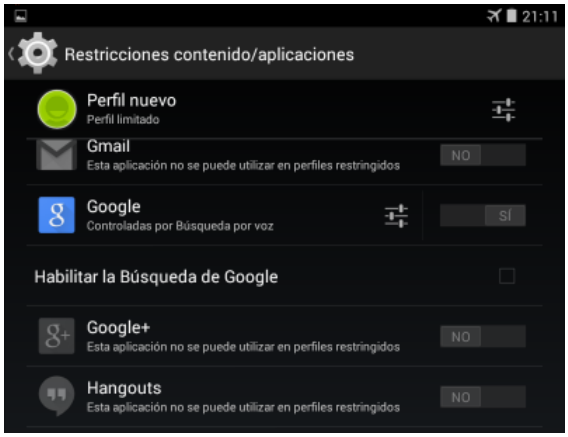
aspectos relacionados con el usuario. Permite por ejemplo añadir (opcionalmente) la cuenta de Google del usuario (ofreciéndose la posibilidad de crear una cuenta de usuario de Google si no se dispone de una), determinar si se permitirá a las apps hacer uso de los servicios de ubicación y con qué precisión, solicita el nombre del usuario para personalizar algunas apps, confirma la aceptación de actualizaciones a través de los servicios de Google, y permite al usuario personalizar la pantalla de inicio.

380. Los usuarios con un perfil limitado asociado pueden disponer de capacidades para modificar algunos ajustes de configuración, como por ejemplo permitir a las apps utilizar la ubicación del dispositivo móvil, definidos durante el proceso de configuración del perfil, junto al nombre asignado a dicho perfil de usuario:



381. El proceso de configuración del perfil limitado también permite establecer qué otras apps, y capacidades de la plataforma móvil Android (como por ejemplo las búsquedas por voz en los servicios de Google), estarán disponibles para dicho perfil de usuario:





382. La implementación multiusuario de Android asigna un identificador (o ID) a cada usuario (y que es independiente de los identificadores o UIDs asignados a las apps a nivel de Linux), empezando por el identificador 0, asignado al usuario propietario.

383. La información de cada usuario se almacena en el directorio "/data/system/users/<ID>", donde se guardan los ajustes de configuración del usuario, las personalizaciones de su pantalla de inicio, y la lista de apps actualmente instaladas y disponibles para ese usuario.

384. Los binarios de las apps se comparten entre los usuarios, para evitar duplicidades y un consumo innecesario de la memoria de almacenamiento, pero el directorio o *sandbox* de trabajo de la app es independiente para cada usuario, obteniéndose una copia del original en el momento de la instalación (o activación) de la app para un usuario concreto.

385. Las capacidades multiusuario de Android modifican el modelo de asignación de identificadores o IDs para las apps descrito en el apartado "5.2.3. Sandbox de ejecución de las apps", ya que al ser instalada para un usuario concreto, cada app recibe un nuevo identificador efectivo combinación del ID de usuario y del ID de la app [Ref.- 157].

386. Una vez se han habilitado diferentes perfiles o usuarios, desde la pantalla de desbloqueo del dispositivo móvil es posible seleccionar con qué usuario se quiere acceder desde la parte inferior central de la misma, seleccionando el icono del usuario elegido:

387. Desde el punto de vista empresarial o corporativo, no se recomienda la compartición de los dispositivos móviles entre distintos usuarios, por lo que se desaconseja el uso de las capacidades para disponer de múltiples perfiles de usuario en Android.

388. En caso de identificarse escenarios donde debe compartirse el uso de una misma tableta Android entre distintos usuarios, se recomienda llevar a cabo un análisis detallado de los requisitos, capacidades y restricciones que se desea imponer a cada usuario, planificar adecuadamente su implementación e investigar minuciosamente las posibles implicaciones de seguridad de la implementación de las capacidades multiusuario para la versión concreta de Android empleada.

5.6 CIFRADO DE DATOS EN ANDROID

5.6.1 CIFRADO DEL DISPOSITIVO MÓVIL

389. Android 4.x dispone de capacidades para el cifrado de los datos almacenados en la memoria interna del dispositivo móvil de forma nativa.

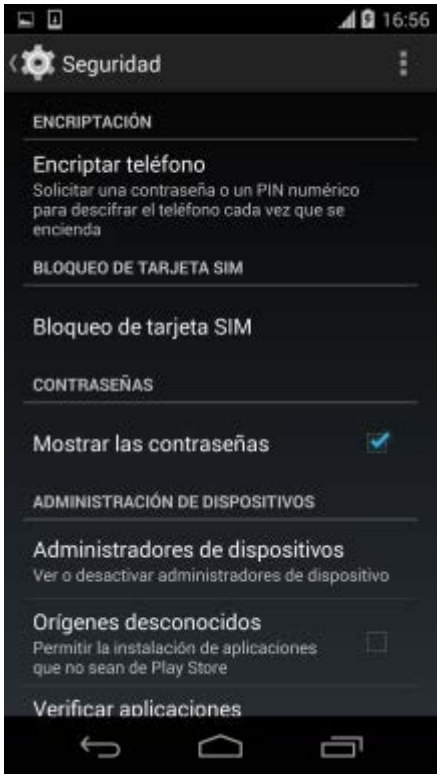
390. Desde la versión 3.0 de Android ("Honeycomb") [Ref.- 31], orientada a dispositivos móviles de tipo tableta, se añadieron capacidades de cifrado nativas a los dispositivos móviles basados en Android [Ref.- 82], junto a otras mejoras en las políticas de cifrado y de contraseñas (complejidad, expiración e histórico).

391. Lógicamente, la opción de cifrado completo del dispositivo móvil también está disponible en versiones posteriores, como Android 4.0 y versiones superiores, para teléfonos móviles o *smartphones*, tanto del teléfono como (potencialmente) de la tarjeta de almacenamiento externa (en aquellos dispositivos móviles que disponen de una tarjeta SD real).

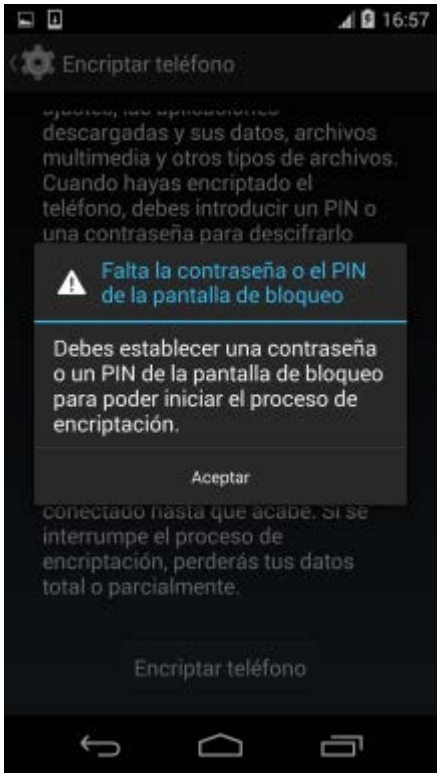
392. Por otro lado, existen numerosas apps de cifrado en Google Play (ej. OpenPGP para Android, AGP[41]) que permiten el cifrado de sus propios datos, como por ejemplo notas, información confidencial o contraseñas, pero no de la totalidad del dispositivo móvil.

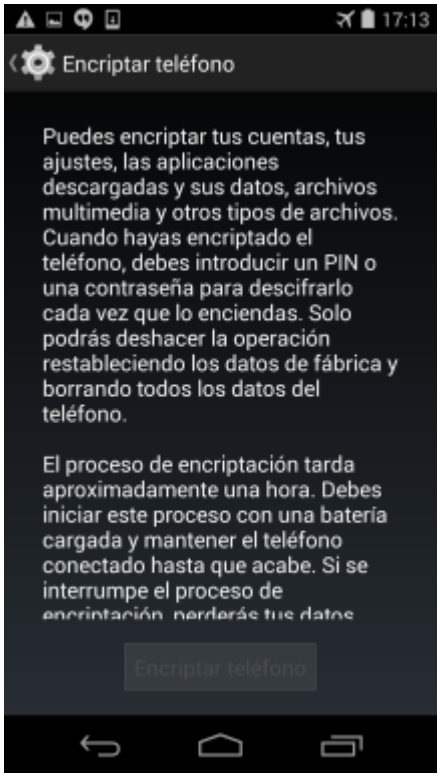
393. La opción "Encriptar teléfono" (o *tablet*) está disponible desde el menú "Ajustes [Personal] - Seguridad [Encriptación]":

[41] https://play.google.com/store/apps/details?id=org.thialfihar.android.apg&hl=es



394. Para poder activar dichas capacidades de cifrado en Android 4.x es necesario establecer un código de acceso en el dispositivo móvil en forma de contraseña o PIN. Asimismo, el dispositivo móvil debe estar conectado a la corriente y cargando la batería, para evitar que se interrumpa el proceso de cifrado sin haberse completado:



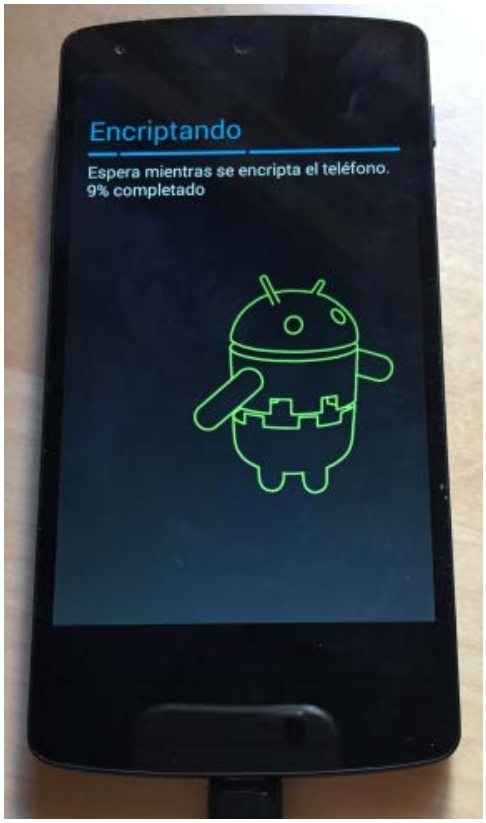


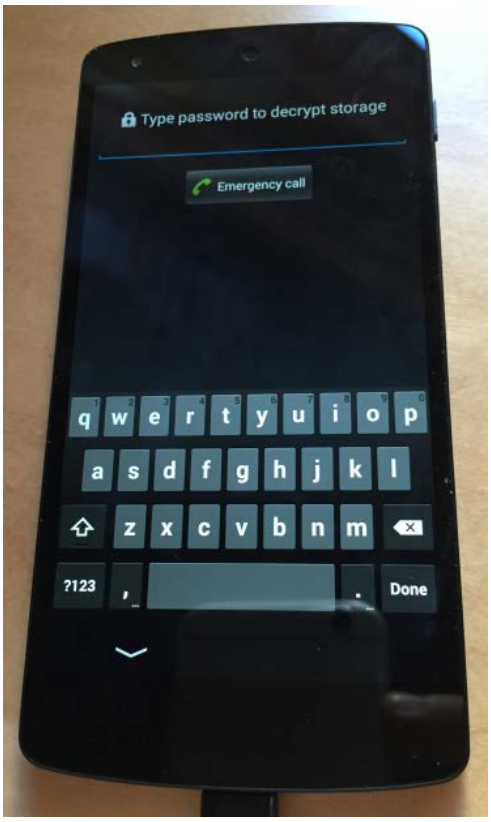
395. Una vez se cumplen los requisitos necesarios, mediante el botón "Encriptar teléfono" es posible comenzar el proceso, siendo necesario confirmar el código de acceso en primer lugar. Durante el proceso el dispositivo móvil se reiniciará en varias ocasiones, y aunque la

información proporcionada indica que el proceso puede tardar 1 hora, en el dispositivo móvil empleado para la elaboración de la presente guía se completó en unos 15-20 minutos aproximadamente:

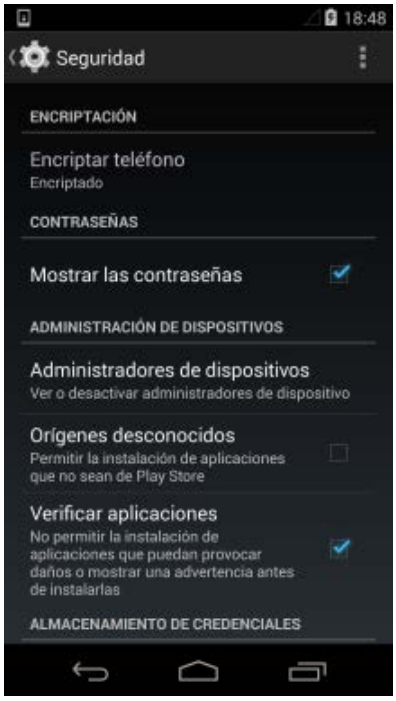
396. En el caso de la implementación de cifrado completo del dispositivo móvil de Android, denominada FDE (*Full Device Encryption*), pese a su nombre, en realidad sólo se cifra la partición o sistema de ficheros con los datos de usuario (*userdata*), correspondiente al punto de montaje "/data", y no toda la memoria del dispositivo móvil.

397. Durante el proceso de arranque, el usuario debe introducir el código de acceso para que se pueda llevar a cabo el proceso de descifrado de la partición de datos de usuario y su montaje, y por tanto, el arranque del sistema operativo:





398. Por otro lado, el proceso es irreversible, siendo únicamente posible deshabilitar el cifrado mediante la restauración del dispositivo móvil a sus ajustes de fábrica (lo que eliminará todos los datos del terminal) y restaurando posteriormente los datos de usuario desde una copia de seguridad. La única opción disponible una vez la memoria del dispositivo móvil ha sido cifrada es la indicación de que la memoria está cifrada ("Encriptado") bajo la opción "Encriptar Teléfono" de los ajustes:



399. La implementación de cifrado del dispositivo móvil (FDE, *Full Device Encryption*) de Android está basada en cryptfs (dm-crypt)[42] empleando AES 128 bits en modo CBC y con ESSIV:SHA256 [Ref.- 155] y PBKDF2 con 2000 iteraciones para la derivación de la clave empleada para cifrar la clave maestra.

400. Desde la versión 4.4 de Android (KitKat) se emplea scrypt en lugar de PBKDF2. Los dispositivos móviles cifrados con versiones previas de Android migran a scrypt en el primer arranque tras actualizar a KitKat [Ref.- 156].

401. Debe tenerse en cuenta que la implementación del cifrado completo del dispositivo móvil (FDE) empleada por Android hace uso del mismo código de acceso tanto para el cifrado como para el desbloqueo del terminal.

402. Este modelo de cifrado ha sido empleado por Android desde los orígenes de FDE (es decir, desde Android 3.0, Honeycomb), y tiene numerosas implicaciones negativas desde el punto de vista de seguridad. Debido a que se emplea el mismo código, y a que los usuarios deben introducir el código de acceso o desbloqueo del terminal en múltiples ocasiones a lo largo del día, tenderán a elegir un código más sencillo y fácil de utilizar, y por tanto de adivinar, y que puede potencialmente ser obtenido mediante técnicas de ataque de fuerza bruta sobre la memoria (o partición de datos) del dispositivo móvil.

403. Por otro lado, el código de cifrado está limitado a 16 caracteres (por diseño de Android [Ref.- 151]), por lo que no es posible hacer uso de frases de paso (*passphrases*) en lugar de contraseñas (*passwords*). Existen herramientas disponibles públicamente para llevar ataques de fuerza bruta sobre la partición de datos del dispositivo móvil y obtener la contraseña de cifrado, y en consecuencia, el código de acceso [Ref.- 132].

404. El uso de scrypt en lugar de PBKDF2 en Android 4.4 (o superior), dificulta ligeramente este tipo de ataques ralentizando su ejecución, especialmente cuando se emplean GPUs (Graphical Processing Units) en lugar de CPUs para los ataques de fuerza bruta [Ref.- 132].

405. Adicionalmente, un potencial atacante podría ver como el usuario teclea el código de acceso en la pantalla del terminal, mediante técnicas de *shoulder surfing*, y obtener a su vez la contraseña de cifrado.

406. Mientras el código de acceso sólo debe proteger frente a ataques *online*, protegido por técnicas que limitan el número de intentos fallidos a través de la pantalla de desbloqueo, la contraseña de cifrado debe también proteger frente a ataques *offline*, dónde es posible probar un mayor número de combinaciones por unidad de tiempo y sin limitaciones.

407. Como resultado, un potencial atacante dispondría del código de acceso que le permitiría tanto desbloquear y acceder al dispositivo móvil, como descifrar los contenidos de una imagen (o copia) de la memoria o ROM del terminal. Esta debilidad fue ya notificada a Google en abril de 2012 mediante el caso (*issue*) 29468 [Ref.- 14].

408. Debe tenerse en cuenta que es posible en Android modificar la contraseña de cifrado (e independizarla del código de acceso) a través de las utilidades de gestión de los volúmenes y particiones del dispositivo móvil, pero para ello es necesario disponer de permisos de root [Ref.- 155]. Por este motivo, esta información sólo se proporciona a modo informativo:

[42] https://source.android.com/devices/tech/encryption/android_crypto_implementation.html

```
# vdc cryptfs changepw <nueva_contraseña>
```

409. Algunas alternativas similares existentes, en forma de apps de Android, como por ejemplo EncPassChanger [Ref.- 153] o Cryptfs Password [Ref.- 154] (que también requieren disponer de permisos de root), permiten establecer dos códigos diferentes (contraseña de cifrado y código de acceso).

410. Debe tenerse en cuenta que al emplear estas herramientas de personalización, cada vez que se modifique el código de acceso del dispositivo móvil será necesario modificar de nuevo la contraseña de cifrado, por lo que sería preferible que el proceso se unificara de forma nativa en Android y automática para el usuario.

411. Se considera que los usuarios podrían aceptar de manera más confortable disponer de un código más complejo y de mayor longitud para el cifrado del dispositivo móvil, que únicamente debe ser introducido una vez durante el proceso de arranque, y otro código menos robusto, que les permita desbloquear y acceder al dispositivo múltiples veces a lo largo del día de manera más cómoda.

412. Por defecto las capacidades de cifrado nativas del dispositivo móvil están deshabilitadas en Android 4.x.

413. Se recomienda habilitar el cifrado completo del dispositivo móvil con el objetivo de evitar ataques de acceso a los datos almacenados en caso en el que un potencial atacante disponga de acceso físico al dispositivo móvil y desconozca la contraseña de acceso.

5.6.2 CIFRADO DE LAS TARJETAS DE ALMACENAMIENTO EXTERNAS

414. Android 4.x dispone (potencialmente) de capacidades para el cifrado de los datos que vayan a ser guardados en tarjetas de almacenamiento externas de forma nativa.

415. Las soluciones de cifrado (ver apartado "5.6.1. Cifrado del dispositivo móvil") deberían contemplar tanto la protección o cifrado de la memoria interna del dispositivo móvil como de las tarjetas de almacenamiento externas.

Nota: el dispositivo móvil empleado para la elaboración de la presente guía (al igual que la mayoría de los dispositivos móviles Nexus de Google recientes) no dispone de capacidades de almacenamiento externas reales, en forma de un *slot* o ranura para tarjetas SD. Por este motivo, las opciones disponibles para el cifrado del terminal en el menú de "Ajustes" no incluyen ninguna referencia al almacenamiento externo.

En el caso de disponer de una tarjeta de almacenamiento externa real, las opciones de configuración de cifrado de la tarjeta SD están disponibles también a través de la sección de ajustes correspondiente: "Ajustes [Personal] - Seguridad [Encriptación] - Encriptar la tarjeta de memoria externa".

416. En los dispositivos móviles dónde no se dispone de capacidades de almacenamiento externas reales, en forma de un *slot* o ranura para tarjetas SD removibles, sin embargo sí se dispone de almacenamiento externo desde el punto de vista de Android. Para ello se crea un espacio de almacenamiento virtual o emulado, en la memoria interna y por tanto no removible, en concreto mediante una partición asociada al punto de montaje "/sdcard", que está asociado a una supuesta tarjeta de almacenamiento externa. Este área de

almacenamiento se emplea como almacenamiento externo, pero realmente hace uso de parte de la memoria interna del dispositivo móvil.

417. La referencia a "/sdcard" en el sistema de ficheros normalmente apunta a "/data/media/0" (y a otras posibles referencias, como "/storage/sdcard0"), es decir, que físicamente se almacena en el mismo volumen o partición de datos o usuario ("/data"). Esta tarjeta SD virtual es accesible desde Windows en formato FAT32, aunque en realidad la partición donde reside hace uso del sistema de ficheros "ext4" (y emplea FUSE para la conversión entre distintos sistemas de ficheros[43]).

418. El almacenamiento externo es uno de los mecanismos disponibles en Android para compartir datos y ficheros entre apps, almacenar contenidos multimedia por parte del usuario, y para compartir datos con un ordenador conectado por USB al dispositivo móvil.

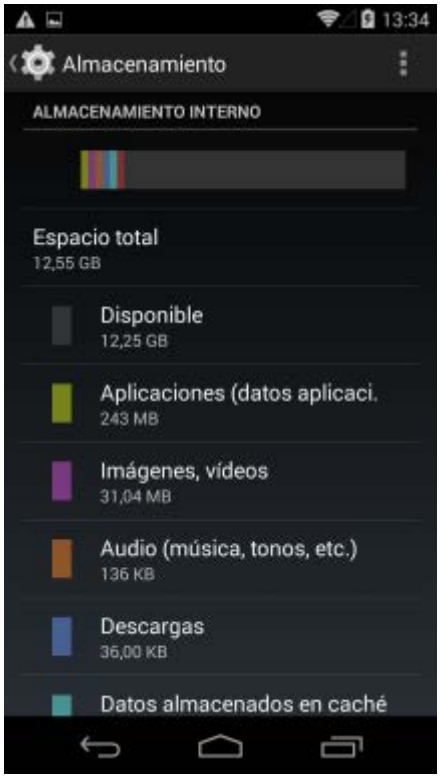
419. Las apps que quieren leer o escribir en el almacenamiento externo deben solicitar los permisos "READ_EXTERNAL_STORAGE" y "WRITE_EXTERNAL_STORAGE" respectivamente[44], siendo únicamente necesario el permiso de escritura para ambas tareas (ya que éste conlleva explícitamente el permiso de lectura).

420. Desde Android 4.4 estos permisos no son necesarios si la app sólo requiere disponer de acceso a ficheros privados de la propia app, mediante el uso de directorios privados a la app dentro del almacenamiento externo.

421. Con el objetivo de evitar el acceso a los datos almacenados en tarjetas externas por parte de un potencial atacante, se recomienda, en el caso de disponer de las capacidades necesarias en el dispositivo móvil y la versión de Android, habilitar esta opción de cifrado.

422. Adicionalmente debe tenerse en cuenta que el sistema de ficheros (FAT o FAT32) empleado por defecto en la tarjeta de almacenamiento externa no establece permisos e impone ninguna restricción, por lo que cualquier app con permisos de acceso sobre la tarjeta SD dispondrá de acceso a todos los datos almacenados en ella (de lectura o de escritura).

[43] http://forum.xda-developers.com/google-nexus-5/general/info-storage-nexus-5-data-info-loss-t2534010
[44] http://developer.android.com/guide/topics/data/data-storage.html#filesExternal



423. La disponibilidad de una tarjeta de almacenamiento externa en el dispositivo móvil (así como la memoria total y disponible en la misma) puede ser confirmada a través del menú "Ajustes [Dispositivo] - Almacenamiento", y concretamente bajo la sección "Tarjeta SD". En caso de no disponer de una, como el dispositivo móvil empleado para la elaboración de la presente guía, únicamente se muestra la sección de "Almacenamiento Interno".

5.7 GESTIÓN DE CERTIFICADOS DIGITALES Y CREDENCIALES EN ANDROID

5.7.1 ALMACENAMIENTO DE CREDENCIALES

424. Android dispone de un repositorio (o almacén) de credenciales, denominado "Almacenamiento de Credenciales", protegido por mecanismos de cifrado, dónde se almacenan los certificados digitales, como por ejemplo los asociados a redes VPN y redes Wi-Fi (ver los apartados correspondientes), o los empleados desde el navegador web, el cliente de correo electrónico y otras apps.

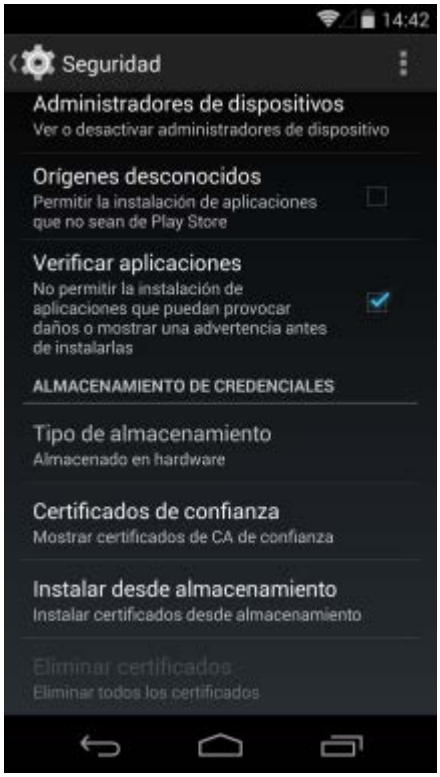
425. Este repositorio de credenciales se conoce oficialmente como el "Android KeyStore" [Ref.-142], y desde Android 4.3 dispone de un interfaz, librería o API asociada para que las apps puedan almacenar certificados digitales, incluso independientes por usuario (en dispositivos Android multiusuario).

426. El concepto de credenciales desde el punto de vista de Android y de este repositorio incluye certificados digitales y, en todo caso, el par de claves pública y privada asociadas a los certificados digitales propios. Oficialmente, este repositorio no proporciona funciones para el almacenamiento de contraseñas, u otras credenciales y secretos por parte de las apps[45] [46].

[45] https://github.com/nelenkov/android-keystore

427. Las opciones existentes oficialmente para el almacenamiento de otros secretos y contraseñas por parte de las apps pasan por hacer uso de las preferencias compartidas (SharedPreferences) de la app [Ref.- 124], o del AccountManager[47] (gestor de cuentas), siempre debiendo ser muy cuidadosos los desarrolladores de apps de Android a la hora de almacenar información sensible en el *sandbox* de la app[48].

428. La sección "Almacenamiento de Credenciales" está disponible desde el menú "Ajustes [Personal] - Seguridad", en la parte inferior:



429. La opción "Tipo de almacenamiento" indica los detalles de implementación del repositorio de credenciales. En el caso del dispositivo móvil bajo estudio, las credenciales se almacenan en un almacén seguro implementado en el hardware del dispositivo: "Almacenado en hardware"[49].

430. Si la implementación del almacén es de tipo hardware, las claves son generadas y almacenadas en dicho almacén seguro, independiente del sistema operativo Android, y no deberían estar accesibles directamente, ni siquiera para el usuario root.

431. La implementación del almacén seguro mediante hardware, por ejemplo en algunos dispositivos móviles Nexus basados en los SoC (System on a Chip) Qualcomm, emplea las capacidades TrustedZone de los procesadores ARM, y en concreto, el Qualcomm Secure Execution Environment (QSEE) [Ref.- 188] [Ref.- 142] . Otras implementaciones son posibles haciendo uso de Secure Elements (SEs), Trusted Platform Modules (TPMs) o Universal Integrated Circuit Cards (UICCs; por ejemplo, una tarjeta SIM).

[46] http://nelenkov.blogspot.com.es/2012/05/storing-application-secrets-in-androids.html
[47] http://developer.android.com/reference/android/accounts/AccountManager.html
[48] http://android-developers.blogspot.com.es/2013/02/using-cryptography-to-store-credentials.html
[49] Es necesario analizar en detalle los componentes hardware del modelo de dispositivo móvil concreto para conocer las capacidades de almacenamiento seguro de credenciales disponibles.

432. Si la implementación del almacén es de tipo software, las claves son cifradas mediante AES [Ref.- 185] con una clave maestra para cada usuario, y almacenadas bajo "/data/misc/keystore/user_N/" (donde por defecto "N" es igual a "0" para el usuario inicial o propietario del dispositivo móvil, es decir, ".../user_0/"). En el siguiente ejemplo el nombre de los ficheros corresponde al nombre asignado al certificado, "raul (DinoSec)":

```
root@hammerhead:/data/misc/keystore/user_0 # ls -l

-rw------- keystore keystore     1300 2015-01-19 12:07
1000_CACERT_raul+P+XDinoSec+Y
-rw------- keystore keystore     1412 2015-01-19 12:07
1000_USRCERT_raul+P+XDinoSec+Y
-rw------- keystore keystore     1652 2015-01-19 12:07
1000_USRPKEY_raul+P+XDinoSec+Y
```

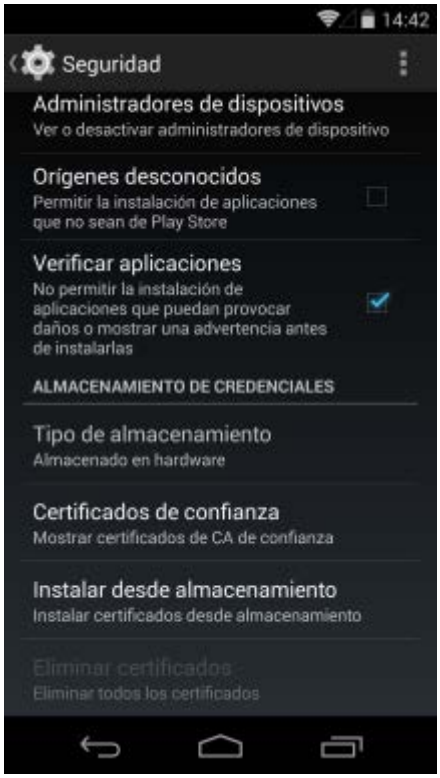
433. La versión 4.4 de Android solucionó una vulnerabilidad de desbordamiento de buffer (buffer overflow) en el KeyStore de Android [Ref.- 143].

5.7.2 CERTIFICADOS DIGITALES DE SISTEMA Y DE USUARIO

434. Los contenidos del repositorio de credenciales pueden ser visualizados tanto desde las aplicaciones que hacen uso de él, como por ejemplo, la configuración de redes VPN (ver apartado "5.17.6. Redes VPN") o de redes Wi-Fi basadas en 802.1x EAP (ver apartado "5.14.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi"), a la hora de seleccionar el certificado de usuario a utilizar y en el caso de los certificados digitales cliente, o desde el certificado de confianza en el caso de los certificados digitales correspondientes a las autoridades certificadoras (CAs, Certification Authorities).

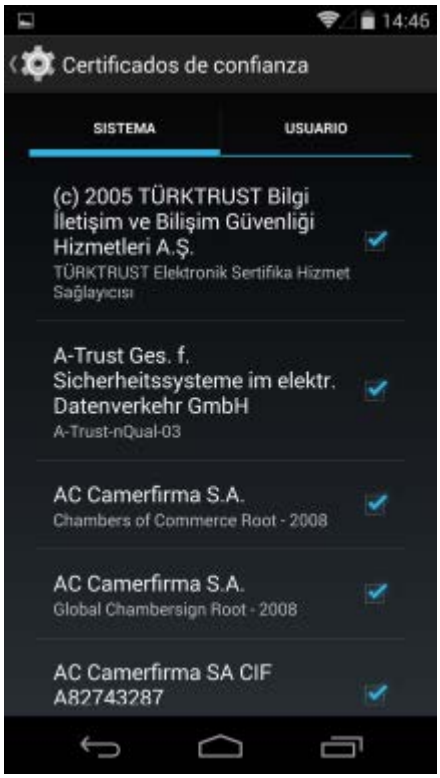
435. En las versiones 2.x de Android, por defecto, no era posible acceder al listado de CAs reconocidas por el dispositivo móvil desde el interfaz gráfico de usuario, y mucho menos disponer de opciones en el interfaz de usuario que permitieran modificar y gestionar la lista de CAs raíz.

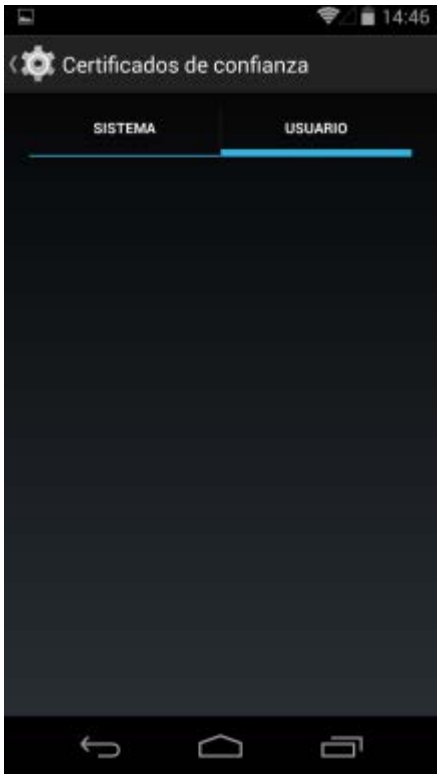
436. Sin embargo, desde la versión 4.0 de Android sí es posible acceder al repositorio de certificados de confianza, tanto de usuario como de sistema, desde la sección "Almacenamiento de Credenciales", disponible a través del menú "Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]", y en concreto, mediante la opción "Certificados de confianza":



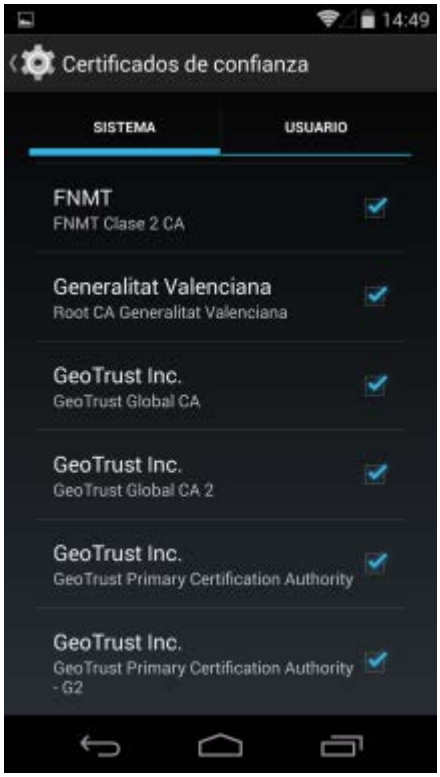
437. Este repositorio de certificados de confianza también se conoce como el "Trust Store" [Ref.- 186] y es un elemento clave para la seguridad de Android.

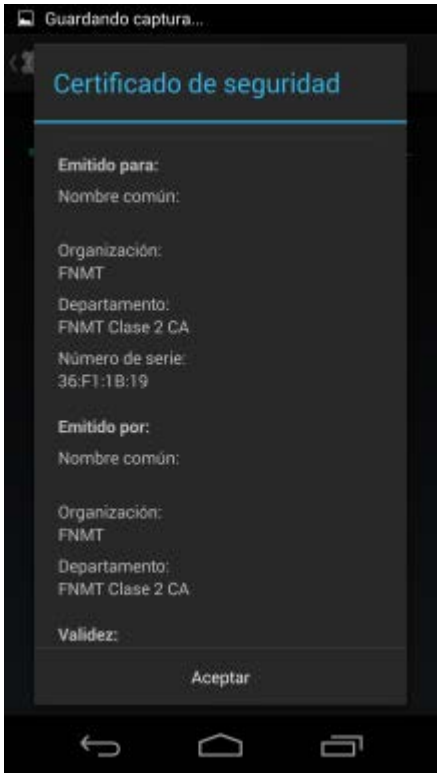
438. Esta sección dispone de dos pestañas, la primera de ellas asociada al "Sistema", es decir, a la lista de autoridades certificadoras (CAs) raíz reconocidas por defecto en esa versión concreta de Android, y la segunda asociada al "Usuario", con los certificados digitales tanto de CAs como personales que han sido añadidos posteriormente por el usuario (vacía por defecto):



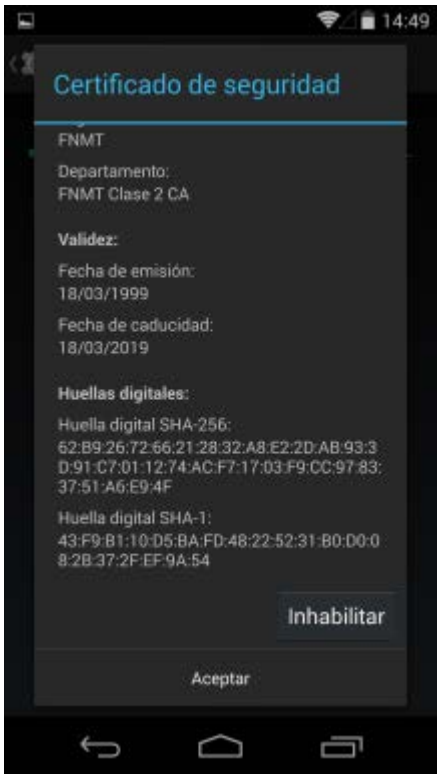


439. Desde la pestaña "Sistema" es posible visualizar la lista completa de CAs de confianza existente por defecto, pudiendo ver todos los detalles de sus certificados al seleccionar cualquiera de las CAs de la lista, así como desactivar de forma independiente cada uno de los certificados raíz de cada CA contenidos en este repositorio:



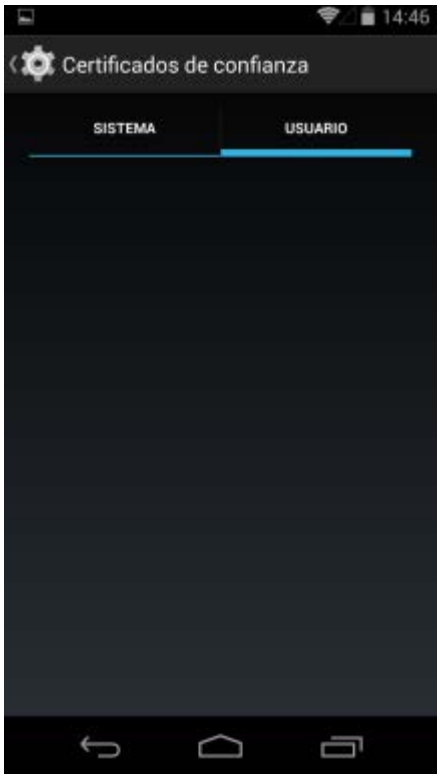


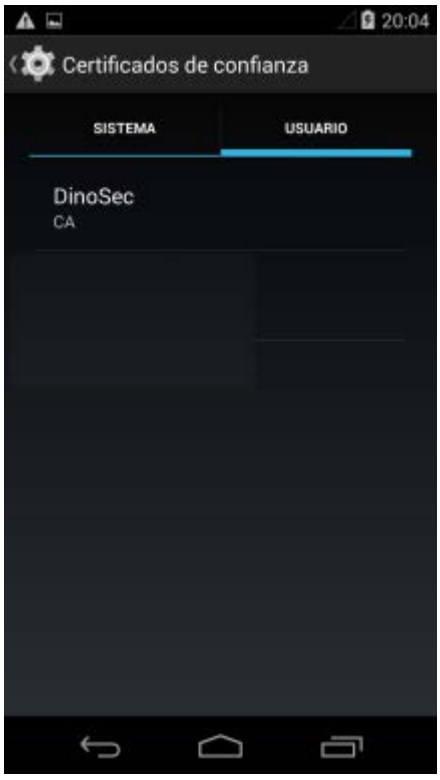
440. Las CAs pueden ser deshabilitadas tanto empleando el cuadro de selección disponible en la parte derecha de cada entrada de la lista, como empleando el botón "Inhabilitar" situado en la parte inferior de la pantalla que muestra los detalles del certificado:



441. En cualquier momento una CA deshabilitada previamente puede volver a ser habilitada, de nuevo, mediante el cuadro de selección disponible en la parte derecha de cada entrada de la lista, o empleando el botón "Habilitar" situado en la parte inferior de la pantalla que muestra los detalles del certificado:

442. La pestaña "Usuario" no contiene ningún certificado digital, para una CA o personal, por defecto. Una vez se importa un certificado (ver apartado "5.7.3. Añadiendo certificados digitales"), los detalles del mismo están disponibles a través de esta pantalla:





443. Mediante el SDK (Software Development Kit) de Android es posible inspeccionar y extraer manualmente desde un ordenador, a través del puerto USB, el conjunto de certificados raíz asociado a las autoridades certificadoras (CAs) existentes por defecto en el dispositivo móvil, accediendo a través de ADB (Android Debug Bridge).

444. La modificación de los certificados digitales de las CAs reconocidas por defecto requiere disponer de un dispositivo móvil Android *rooted*, por lo que en su lugar se recomienda hacer uso del interfaz de usuario disponible para estas gestiones desde Android 4.x (descrito previamente).

445. El directorio "/system/etc/security/cacerts" contiene un fichero por cada uno de los certificados digitales asociados a las CAs reconocidas por Android, en lugar de estar todos ellos contenidos en un único fichero contenedor "cacerts.bks" (BKS, BouncyCastle Key Store [Ref.- 27]), dentro del mismo directorio, tal como ocurría en versiones de Android previas a la versión 4.x:

```
shell@hammerhead:/system/etc/security $ ls -l
...
drwxr-xr-x root     root              2014-05-07 21:39 cacerts
-rw-r--r-- root     root         1433 1970-01-31 13:11 otacerts.zip

shell@hammerhead:/system/etc/security $ cd cacerts
shell@hammerhead:/system/etc/security/cacerts $ ls
...
00673b5b.0
02b73561.0
052e396b.0
...
```

446. El nombre de cada fichero corresponde al *hash* del certificado digital que contiene [Ref.- 44], y mediante herramientas estándar, como por ejemplo openssl, es posible añadir nuevos certificados (en dispositivos móviles Android *rooted*).

447. Para poder inspeccionar el contenido de cada uno de estos ficheros "*.0" es simplemente necesario abrirlos con un editor de texto, ya que contienen el certificado digital en formato PEM (base64), junto a la representación del mismo en ASCII para poder ver sus detalles:

```
-----BEGIN CERTIFICATE-----
MIIEIDCCA...jVaMaA==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            34:4e:d5:57:20:d5:ed:ec:49:f4:2f:ce:37:db:2b:6d
...
```

448. Por tanto, este directorio contiene la lista de todos los certificados digitales raíz con las CAs disponibles por defecto en Android, y contiene exactamente 156 entradas para la versión 4.4.4 (KTU84P) de Android.

449. Desde el punto de vista de seguridad, se recomienda evaluar la necesidad de confiar en todas y cada una de las CAs disponibles por defecto en Android, gestionadas por empresas

privadas de referencia en la industria, gobiernos, empresas privadas menos conocidas e institutos de investigación, y deshabilitar todas aquellas que no se consideran de confianza [Ref.- 189].

450. Por ejemplo, de éstas, 15 CAs raíz todavía hacen uso de un certificado digital basado en una clave RSA de 1.024 bits, longitud considerada insuficiente actualmente (desde finales del año 2013[50]), recomendándose al menos el uso de claves de 2.048 bits. Por otro lado, 6 CAs raíz todavía hacen uso de un certificado digital basado en una firma o *hash* obtenida mediante MD5 (considerado insuficiente desde hace años), mientras que 115 CAs raíz todavía hacen uso de firmas obtenidas mediante SHA-1 (considerado insuficiente más recientemente, recomendándose la utilización de SHA-256).

451. Adicionalmente, como se ha descrito previamente, desde Android 4.0 se extiende la posibilidad de añadir nuevos certificados al repositorio de certificados de confianza ("Trust Store") [Ref.- 186] del sistema (certificados existentes por defecto). Estos se almacenan bajo "/data/misc/keychain", en los directorios "cacerts-added" (que contiene los certificados digitales añadidos por el usuario, visibles desde la pestaña "Usuario") y "cacerts-removed" (que contiene los certificados digitales de sistema deshabilitados por el usuario, gestionados desde la pestaña "Sistema"), y complementan al directorio que almacena los certificados del sistema descrito previamente, "/system/etc/security/cacerts":

```
shell@hammerhead:/data/misc/keychain/cacerts-added $ ls -l
-rw-r--r-- system   system        883 2015-01-19 22:07 17f1599a.0
-rw-r--r-- system   system        712 2015-01-20 14:01 9a5ba575.0

shell@hammerhead:/data/misc/keychain/cacerts-removed $ ls -l
ls -l
-rw-r--r-- system   system       1023 2015-01-22 11:35 84cba82f.0
-rw-r--r-- system   system        979 2015-01-22 11:35 c3a6a9ad.0
```

452. Debido a que la partición de sistema ("/system") dónde se almacena el repositorio de certificados de confianza del sistema es de sólo lectura, cuando se deshabilita un certificado digital éste no puede ser eliminado, sino que en su lugar se incluye en el directorio "cacerts-removed" bajo "/data/misc/keychain".

453. Por otro lado, desde Android 4.1 se extienden las capacidades de gestión de la confianza depositadas en el repositorio de certificados de confianza del sistema mediante listas negras (*blacklisting*) [Ref.- 187], que afectan tanto a apps como al navegador web y componentes WebView.

454. Se dispone de dos listas negras de sistema para añadir las claves públicas de CAs comprometidas, y los números de serie de certificados digitales de entidades finales (End Entity, EE) comprometidos. Ambas listas son almacenadas tanto en la base de datos de la app "Ajustes", como en ficheros bajo "/data/misc/keychain":

```
- CAs certificates blacklist: /data/misc/keychain/pubkey_blacklist.txt
- EE serial numbers blacklist: /data/misc/keychain/serial_blacklist.txt
```

[50] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

455. El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi (o en redes VPN), se detalla en el apartado "5.14.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi" (y en los apartados correspondientes, VPN).

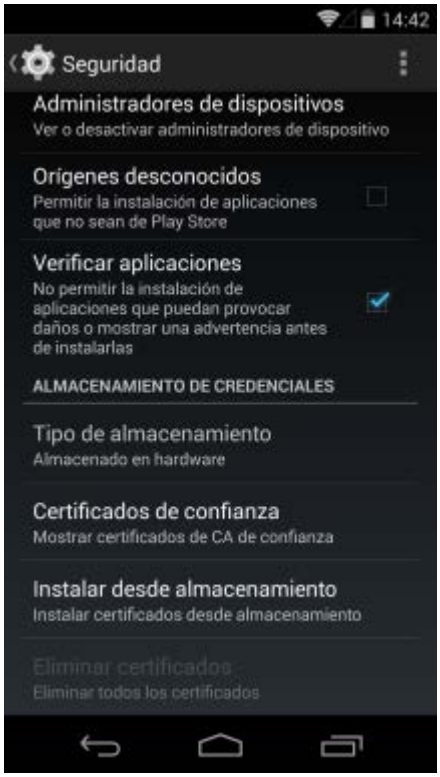
456. Las implicaciones del uso de certificados digitales en funciones de seguridad críticas requiere que el propietario del dispositivo móvil sea muy cuidadoso a la hora de añadir nuevos certificados digitales al dispositivo móvil, y especialmente, al almacén de certificados raíz (o autoridades certificadoras reconocidas).

5.7.3 AÑADIENDO CERTIFICADOS DIGITALES

457. Android permite añadir al dispositivo móvil, o importar, nuevos certificados digitales, tanto correspondientes a una autoridad certificadora (CA), raíz o intermedia (referenciados como raíz por simplificar), como de cliente o personales, complementando así los existentes por defecto.

5.7.3.1 AÑADIENDO CERTIFICADOS DIGITALES RAÍZ

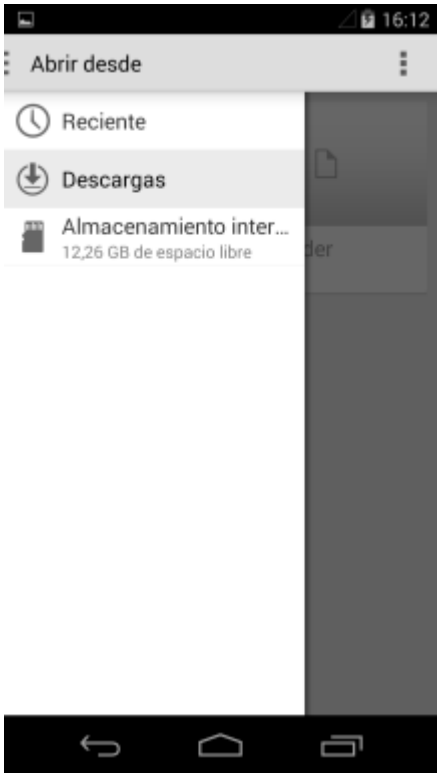
458. Los certificados digitales raíz asociados a una nueva CA pueden ser obtenidos (e importados), por ejemplo, desde un sitio web o desde el almacenamiento interno, o la tarjeta de almacenamiento externa, a través de la opción "Instalar desde almacenamiento" disponible desde el menú "Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]"[51]:

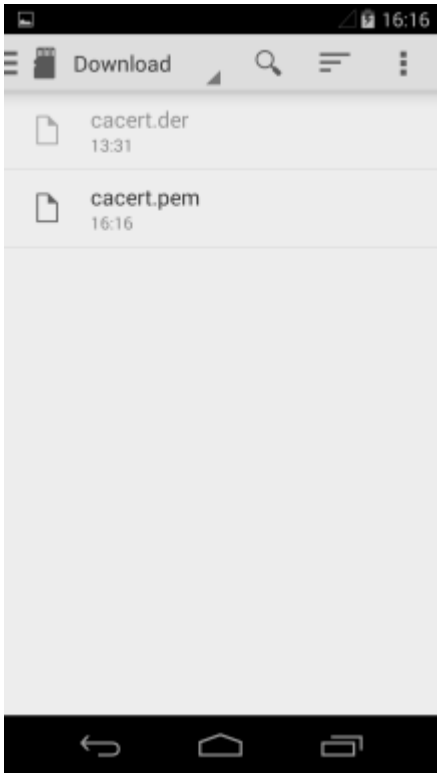


459. Si el certificado digital es obtenido desde la web, por ejemplo a través del navegador web existente por defecto, Chrome, y la extensión del fichero no es reconocida como un

[51] En versiones previas de Android (2.x) el fichero del certificado digital debeía almacenarse directamente en el directorio raíz del almacenamiento interno del dispositivo móvil (o tarjeta SD), no en un subdirectorio.

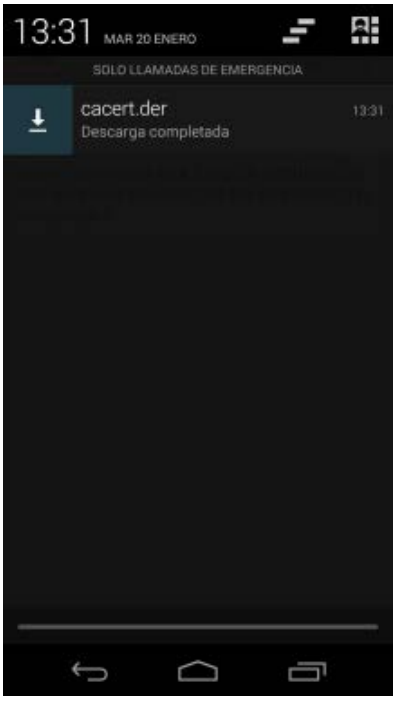
certificado digital válido, Android lo almacenará en la carpeta "Descargas" (o "Download", dentro del almacenamiento interno):

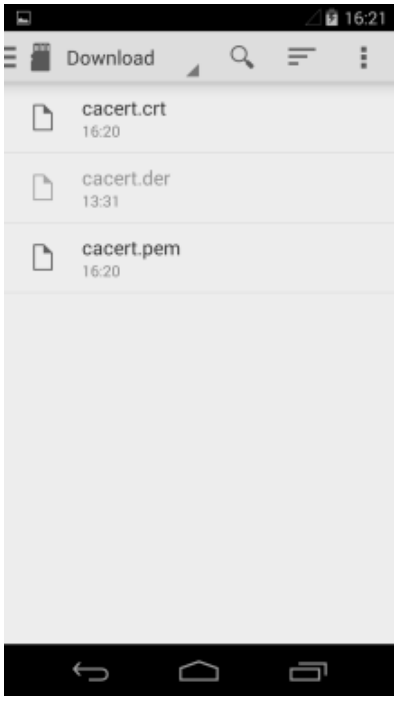




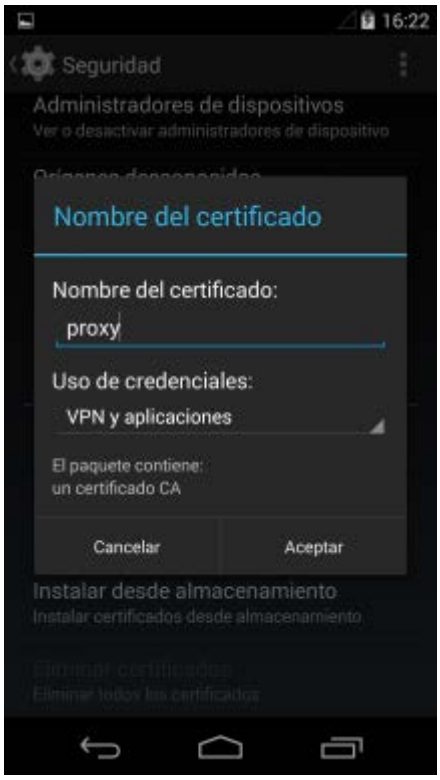
460. Sin embargo, si el certificado digital es obtenido desde la web y la extensión del fichero es reconocida como un certificado digital válido, Android presentará al usuario directamente la ventana para importar el certificado digital en el dispositivo móvil:

461. Para poder proceder a su instalación (tanto directamente desde la web, como desde la tarjeta de almacenamiento), el certificado digital puede estar tanto en formato DER (binario) como PEM (ASCII, en base64), pero debe tener obligatoriamente una extensión válida reconocida por Android, como ".pem", ".cer" o ".crt" (no siendo ".der" una extensión válida en Android) [Ref.- 182]:





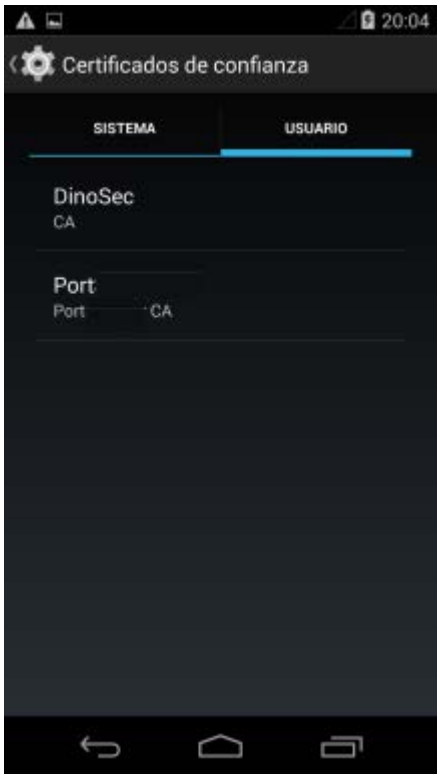
462. Al seleccionar el fichero correspondiente al certificado digital se solicitará al usuario un nombre para su identificación, y el propósito del mismo: "VPN y aplicaciones" o "Wi-Fi".



Nota: los certificados raíz importados mediante estos métodos (desde Android 4.0) no sólo afectan a las conexiones Wi-Fi y a las redes VPN que hacen uso de certificados digitales, sino también a otro tipo de conexiones, como por ejemplo sesiones web autentificadas y cifradas mediante HTTPS, establecidas desde el navegador web o el cliente de correo electrónico, o cualquier otra app cliente, de ahí que la categoría para las redes VPN se denomine "VPN y aplicaciones" [Ref.- 185].

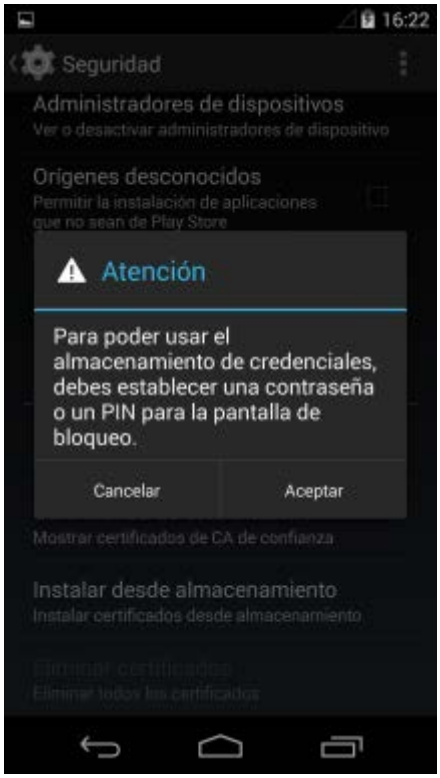
463. El proceso de instalación del nuevo certificado digital no muestra los detalles del mismo, por lo que es muy importante ser especialmente cuidadoso a la hora de importar nuevos certificados, especialmente los descargados directamente desde la web, y verificar posteriormente desde el repositorio de credenciales todos los detalles del certificado recién importado.

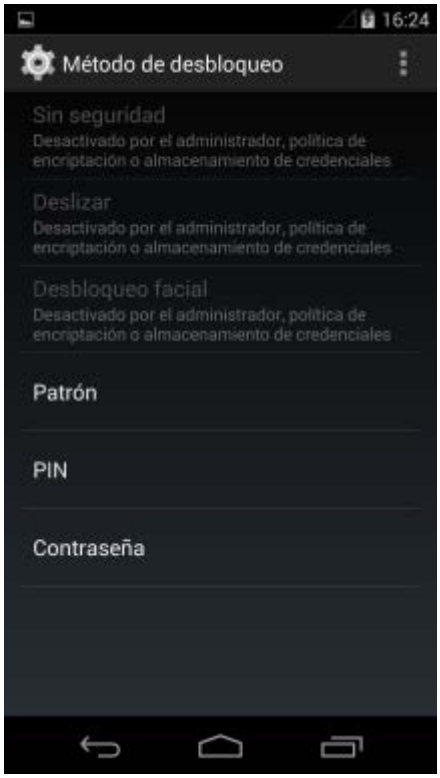
464. El nombre empleado para la identificación de certificados digitales correspondientes a una CA no es mostrado posteriormente a través del interfaz de usuario, ya que en su lugar se muestran en la pestaña "Usuario" los detalles de la organización y del nombre común (CN), en ese orden, que han sido extraídos directamente del certificado. Mediante la selección del certificado digital es posible ver todos sus detalles:



465. Para poder empezar a hacer uso del almacén de credenciales es necesario establecer un código de acceso (ver apartado "5.4.2. Código de acceso al dispositivo móvil") para la pantalla de desbloqueo del dispositivo móvil, en caso de no disponer de una actualmente[52]. Las únicas opciones permitidas como código de acceso para poder hacer uso del repositorio de credenciales son "Patrón", "PIN" o "Contraseña" (descartándose el no seleccionar ningún mecanismo de seguridad, deslizar simplemente el icono del candado, o el uso del desbloqueo facial, debido a su reducido nivel de seguridad):

[52] En versiones previas de Android (2.x) el repositorio de credenciales hacía uso de una contraseña independiente del código de acceso empleado para proteger la pantalla de desbloqueo del dispositivo móvil.

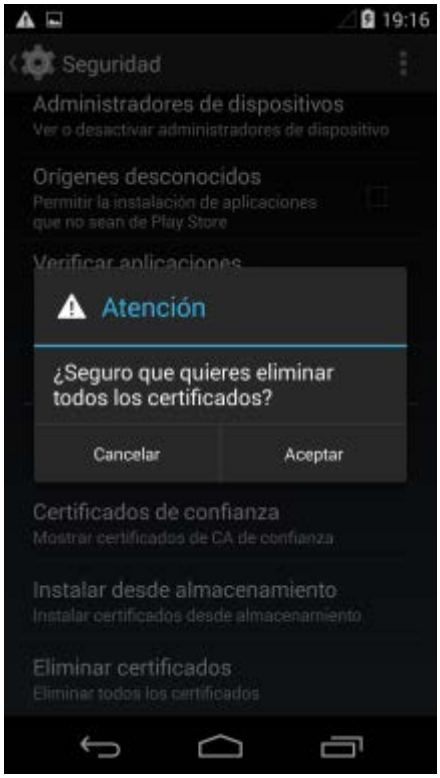




466. El certificado digital es importado en la pestaña "Usuario", aunque se trate de un certificado digital correspondiente a una CA, ya que ha sido añadido a posteriori por el usuario y no forma parte de la configuración por defecto del sistema (pestaña "Sistema").

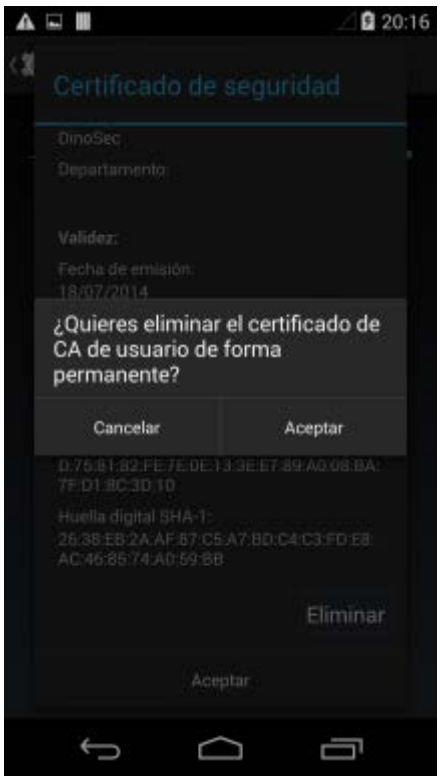
Nota: Android permite importar un mismo certificado digital raíz en múltiples ocasiones, pero en el listado de certificados de confianza, pestaña "Usuario", sólo aparecerá una vez el certificado digital (independientemente del nombre proporcionado al importarlo).

467. Una vez el certificado digital ha sido instalado, la opción "Eliminar certificados" (situada en la parte inferior) es activada en caso de que se quiera eliminar dicho certificado. Sin embargo, esta opción sólo permite eliminar todos los certificados existentes en el repositorio de credenciales simultáneamente, y no de manera selectiva. Es decir, esta opción permite resetear el repositorio de credenciales para volver a hacer uso del mismo desde su estado original:

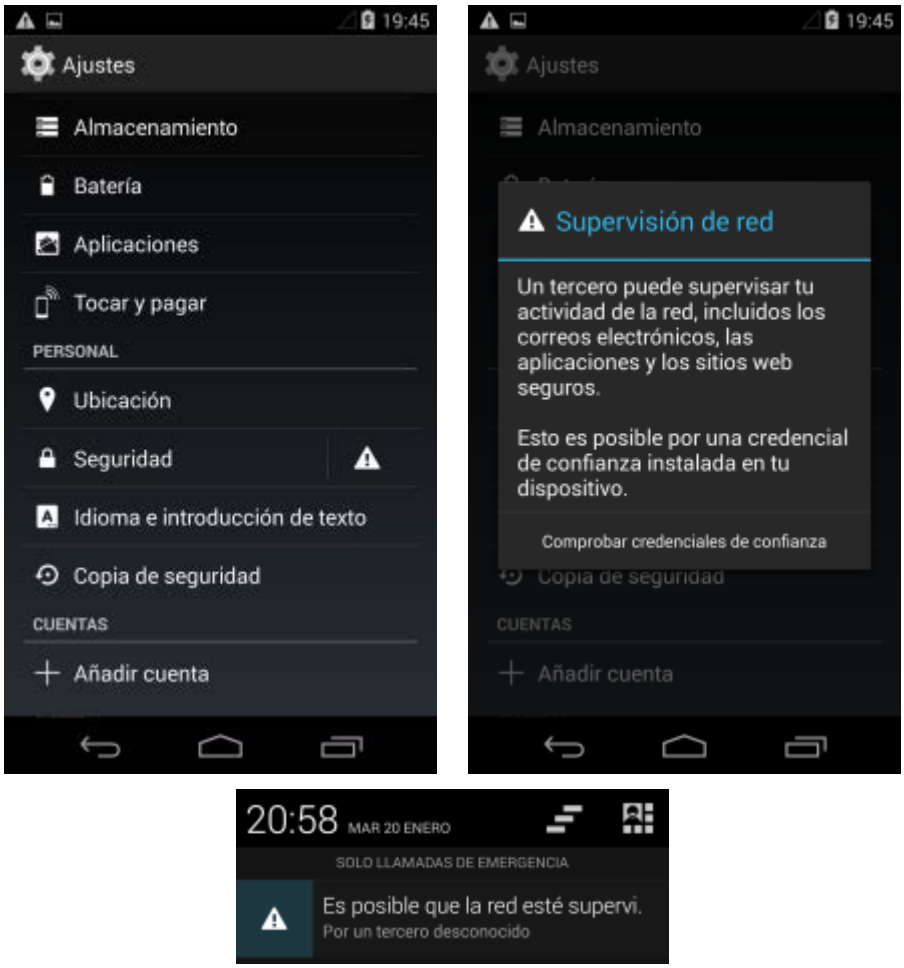


468. Sólo tras eliminar todos los certificados previamente importados (resetear el repositorio de credenciales) sería posible volver a no hacer uso de un código de acceso en el dispositivo móvil (opción no recomendada desde el punto de vista de seguridad).

469. Para eliminar el certificado digital añadido recientemente de manera selectiva es necesario acceder a la lista de certificados de confianza, y desde la pestaña "Usuario", ver los detalles del mismo, pudiendo hacer uso del botón "Eliminar" disponible en la parte inferior:



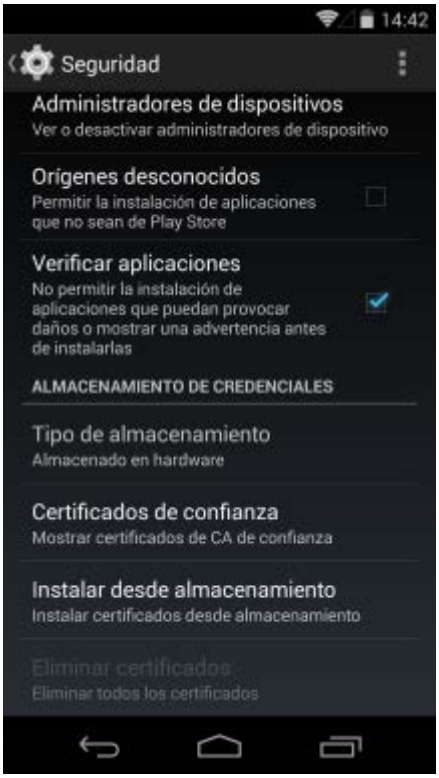
470. Tras llevar a cabo la instalación de un certificado digital asociado a una CA, la sección "Seguridad" del menú "Ajustes" muestra un triángulo de aviso. Asimismo, se muestra al usuario de manera permanente una notificación a través de la barra superior de menú. Al seleccionar el triángulo se informa al usuario de que se ha instalado una nueva CA, lo que puede permitir a un tercero supervisar las actividades del usuario mediante la intercepción de su tráfico de red cifrado:



5.7.3.2 AÑADIENDO CERTIFICADOS DIGITALES CLIENTE

471. Los certificados digitales cliente (o de usuario[53]) asociados, por ejemplo a redes VPN o redes Wi-Fi, pueden ser obtenidos (e importados), por ejemplo, desde un sitio web o desde el almacenamiento interno, o desde la tarjeta de almacenamiento externa, a través de la opción "Instalar desde almacenamiento" disponible desde el menú "Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]" (ver restricciones en el apartado previo):

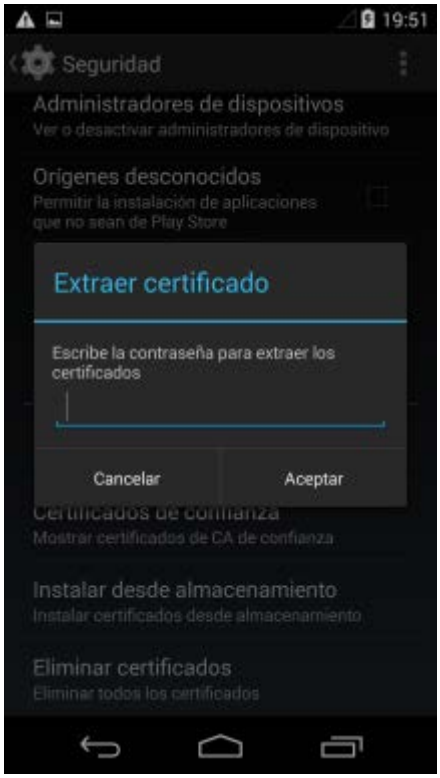
[53] Se hace uso del término certificado digital cliente para referirse a los sertificados empleados para la autentificación del usuario, en lugar de emplearse el término certificado digital de usuario, con el objetivo de evitar confusiones con la pestaña "Usuario" de Android, que muestra tanto certificados cliente como de CAs.



472. Para poder proceder a su instalación, el certificado digital cliente debe estar en formato PKCS#12, con una extensión válida reconocida por Android, como ".p12" o ".pfx" [Ref.-182].

473. Al igual que en el caso de los certificados digitales raíz (ver apartado previo), Android solicitará al usuario establecer una contraseña o código de acceso en el dispositivo móvil para poder hacer uso del repositorio de credenciales, si aún no se ha establecido una.

474. Al seleccionar el fichero correspondiente al certificado digital cliente se solicitará al usuario la contraseña que fue empleada para proteger el fichero PKCS#12 que contiene el certificado digital y la clave privada, y poder así extraer los certificados del fichero:



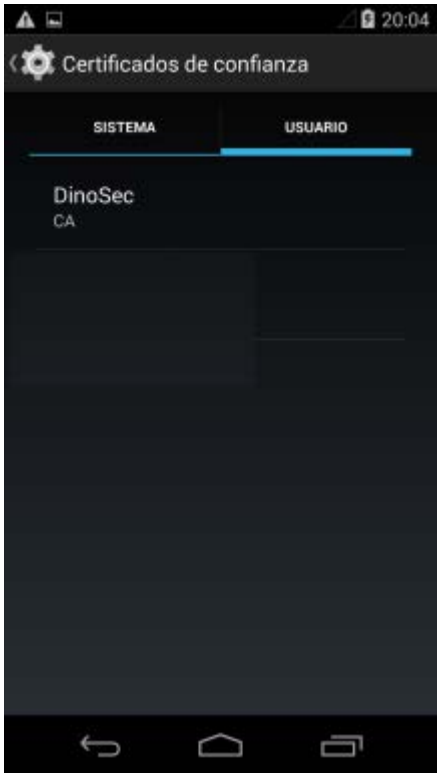
475. Tras extraer el certificado digital cliente (que contiene la clave pública), y la clave privada asociada (y opcionalmente, el certificado de la CA que lo ha emitido), se solicitará al usuario un nombre para su identificación (mostrándose por defecto como nombre el identificador local de la clave, "localKeyID"), y el propósito del mismo: "VPN y aplicaciones" o "Wi-Fi".

476. Se recomienda proporcionar un nombre de certificado que permita la identificación del mismo de forma sencilla desde las aplicaciones cliente que hacen uso de éste. Este nombre

será mostrado posteriormente al seleccionar el certificado digital cliente, por ejemplo, en el proceso de configuración de una red Wi-Fi Empresarial o de una red VPN.

Nota: Android permite importar un mismo certificado digital cliente en múltiples ocasiones, apareciendo múltiples veces en el listado de certificados digitales cliente (o de usuario) disponible a la hora de hacer uso del mismo, por ejemplo, al configurar una red Wi-Fi Empresarial. Cada una de las instancias del certificado digital aparecerá con el nombre proporcionado al importarlo, y en el caso de duplicar dicho nombre durante el proceso de importación, se sobrescribirá la entrada existente previamente.

477. Si se incluye un certificado de una CA junto con el certificado digital cliente, éste se instala de forma simultánea. El certificado digital correspondiente a la CA emisora del certificado digital cliente, si está incluido en el fichero PKCS#12, es también importado en la pestaña "Usuario"[54], al tratarse de un certificado digital correspondiente a una CA, y que ha sido añadido a posteriori por el usuario (y que por tanto no forma parte de la configuración por defecto del sistema, pestaña "Sistema"):

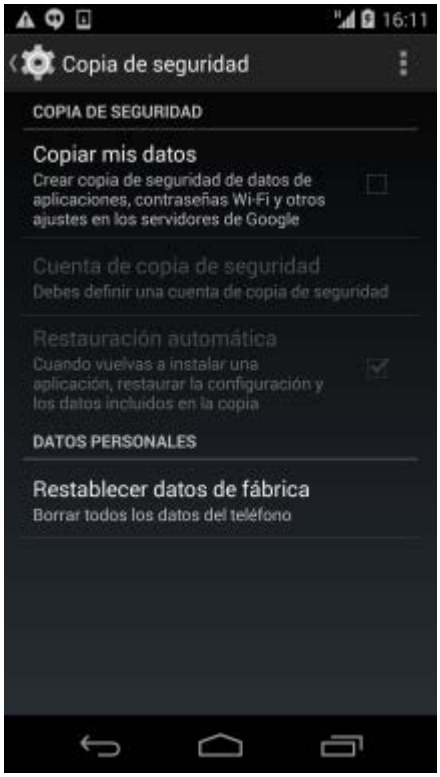


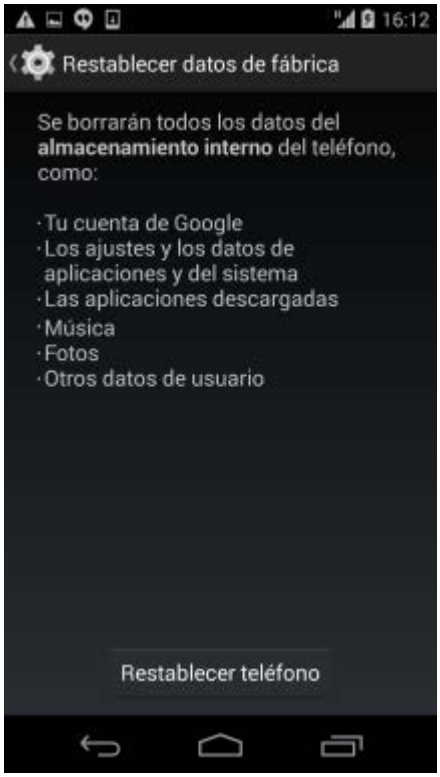
478. El certificado digital cliente añadido recientemente no es visible desde esta sección de los ajustes de configuración, siendo necesario para su visualización acceder desde las aplicaciones que hacen uso de él, como por ejemplo, la configuración de redes VPN o de redes Wi-Fi basadas en 802.1x EAP, y seleccionar el certificado digital cliente (o de usuario) a utilizar.

[54] A diferencia de como ocurría en versiones previas de Android (2.x), el certificado digital importado (ya sea de una CA o personal) no es eliminado de la tarjeta de almacenamiento externa una vez se ha completado la operación de importación.

5.8 ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

479. Android proporciona capacidades locales para la eliminación de todos los datos almacenados en el dispositivo móvil a través del menú "Ajustes [Personal] - Copia de seguridad", bajo la sección "Datos personales" y la opción "Restablecer datos de fábrica":





480. El proceso de restablecimiento eliminará todos los datos del teléfono, incluyendo cuentas de Google, configuración y datos de apps y del sistema, así como apps de terceros previamente descargadas e instaladas. No se eliminará el software del sistema operativo ni las actualizaciones de sistema ya aplicadas, es decir, el propio Android, ni los datos de las tarjetas de almacenamiento externas.

481. Para confirmar esta operación crítica es necesario introducir el código de acceso, y aceptar una última pantalla de confirmación que confirma que se borrarán todos los datos.

482. Estas capacidades de borrado de datos local también pueden ser activadas tras llevarse a cabo un número determinado de intentos de acceso incorrectos, pudiendo configurarse a través de las políticas de seguridad de los mecanismos de gestión empresarial de dispositivos móviles Android (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android") [Ref.- 38].

483. Existen apps disponibles en Google Play, como Locker[55] (app de código abierto que debe instalarse como app administrador del dispositivo), que permiten configurar también este mecanismo de borrado localmente, sin hacer uso de una solución de gestión empresarial de dispositivos móviles.

484. Inicialmente Android no proporcionaba capacidades remotas para la eliminación de todos los datos almacenados en el dispositivo móvil en caso de que el mismo se encontrase en manos de un potencial atacante, proceso conocido como *wipe* (limpieza de datos). Sin

[55] https://play.google.com/store/apps/details?id=net.zygotelabs.locker

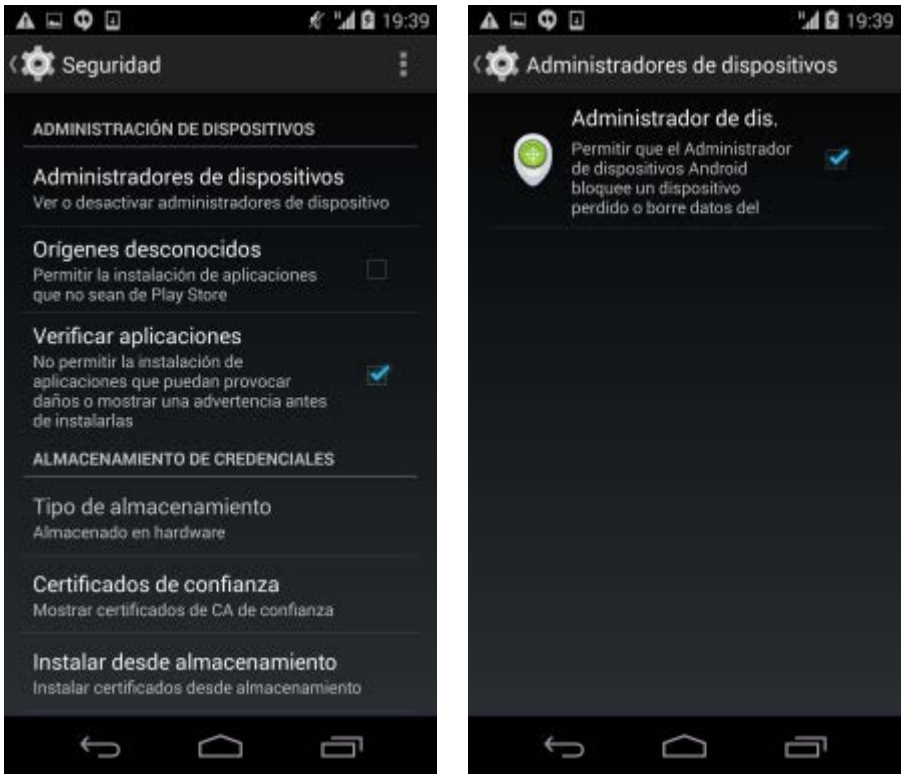
embargo, desde la versión 2.2 de Android [Ref.- 34], estas capacidades están disponibles mediante las distintas soluciones de gestión empresarial de dispositivos móviles basados en Android.

485. Tal y como se mencionaba en el apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android", desde la versión 2.2 de Android, los administradores de un dominio Google Apps (ediciones *Premier* o *Business*, *Government* o *Education*) disponen de capacidades para borrar de forma remota los datos del dispositivo móvil (wipe), en caso de haber sido perdido o robado [Ref.- 88].

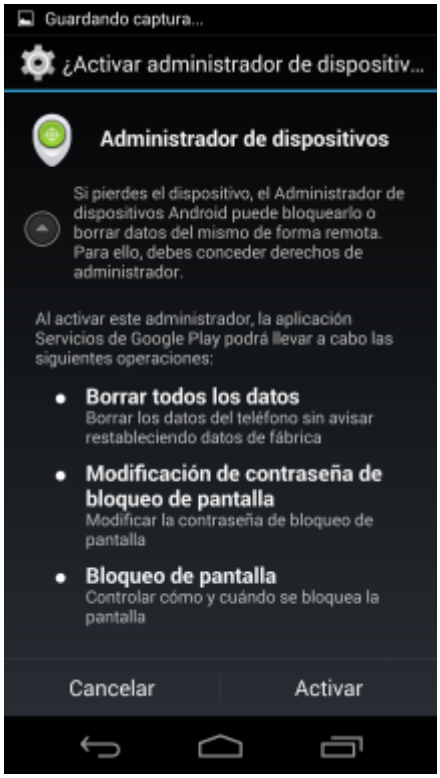
486. Igualmente ese apartado describe la gestión de dispositivos móviles Android a través de Microsoft Exchange y como esta solución también proporciona capacidades similares de borrado de datos remoto (*wipe*) [Ref.- 35].

487. Para que estas capacidades estén disponibles es necesario definir a la app de gestión asociada como aplicación administrador del dispositivo móvil, y que así pueda hacer uso del interfaz "Device Administrator API" y controlar ciertos elementos de seguridad del terminal, como por ejemplo la longitud de la contraseña o el borrado remoto de datos [Ref.- 34].

488. Las aplicaciones (o cuentas) habilitadas como administradores del dispositivo móvil están disponibles desde el menú "Ajustes [Personal] - Seguridad [Administración de Dispositivos] - Administradores de dispositivos":



489. Las aplicaciones administradores del dispositivo móvil pueden ser activadas o desactivadas en función de las necesidades del usuario. Antes de su ejecución, siempre verificarán si están activadas, y en caso de no estarlo, solicitarán al usuario su activación:



490. El administrador de dispositivos existente por defecto en Android 4.4 (y disponible para otras versiones de Android a través de actualizaciones de los servicios de Google Play), que permite el borrado remoto de datos, ha sido descrito en detalle en el apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android".

5.9 CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL

491. El dispositivo móvil está configurado por defecto con valores fijados por el fabricante del sistema operativo, el fabricante del *hardware* o el operador de telefonía móvil, que pueden desvelar detalles del terminal o de su propietario.

492. Para evitar la revelación de información sensible, se recomienda modificar esos valores existentes por defecto por valores elegidos por su propietario.

493. El proceso inicial de instalación y configuración del dispositivo móvil (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial") tiene una influencia muy limitada sobre los valores existentes por defecto y utilizados en diferentes servicios y tecnologías.

494. El nombre del dispositivo móvil Android, o *hostname* al tratarse de un dispositivo Linux, no puede ser fijado a través de los menús de configuración. Su valor por defecto (desde Android 2.2) es "android-CÓDIGO", dónde "CÓDIGO" es un valor de 16 caracteres hexadecimales (ver el análisis de la propiedad "net.hostname" posteriormente; por ejemplo "android-9f6edb6be8c72475").

495. El código corresponde al identificador de Android (ANDROID_ID), un valor de 64 bits (16 caracteres hexadecimales) generado aleatoriamente en el primer arranque del dispositivo móvil y que permanece constante durante toda la vida del dispositivo [Ref.-47], es decir, hasta que se reinstale o se restablezcan los valores de fábrica.

496. Originalmente, y desafortunadamente, el nombre del dispositivo móvil, qué también es empleado como nombre para el servicio DNS (*Domain Name System*), hacía uso del

carácter "_" (*underscore*), qué no es un carácter válido según el estándar del protocolo DNS y los servicios de resolución de nombres [Ref.- 89]. A partir de Android 4.0 ya se hace uso de un guión "-" en su lugar.

497. Únicamente los dispositivos móviles Android dónde se ha realizado el proceso de *rooting* permiten la modificación del nombre del dispositivo móvil (por ejemplo, mediante el comando "hostname" de Linux, o equivalente (ver abajo), y la modificación de los scripts de arranque[56]) [Ref.- 89], pese a tratarse de una característica solicitada a Google desde enero de 2010.

498. Para ello es necesario, como root (su), ejecutar los siguientes comandos en un terminal, empleados para obtener y fijar el nombre del dispositivo móvil Android, aunque el cambio no persistirá tras reiniciar el dispositivo (salvo que se añada a los scripts de arranque):

```
$ getprop net.hostname
android-<CODIGO-NUMERICO>
$ su
# setprop net.hostname NUEVO-NOMBRE
```

499. Las acciones de consulta también pueden ser llevadas a cabo a través del modo de depuración de Android y la utilidad "adb", mediante la ejecución del siguiente comando, por ejemplo, desde Windows:

```
C:\> adb.exe shell getprop net.hostname
android-9f6edb6be8c72475
C:\> adb.exe root
adbd cannot run as root in production builds
```

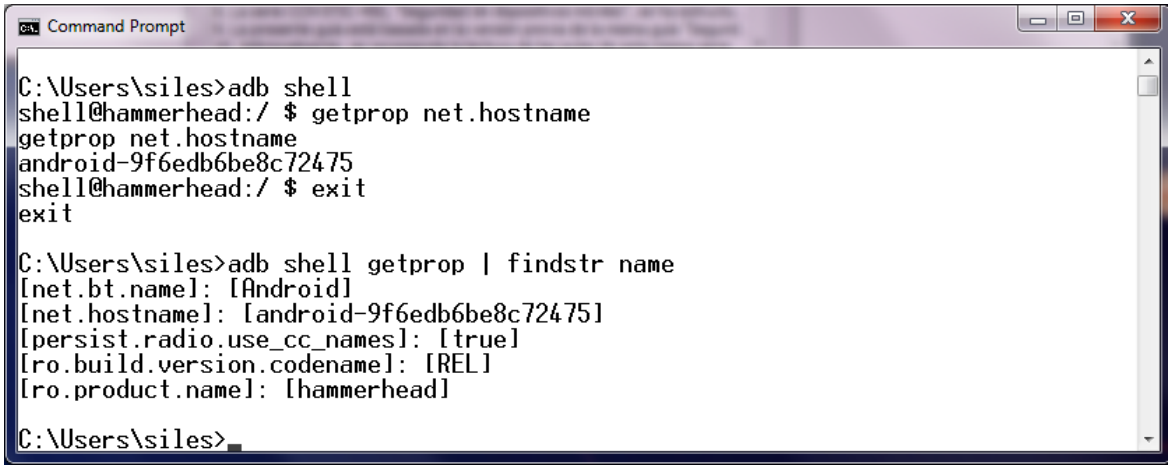
500. La operación de modificación del nombre no se puede llevar a cabo con "adb" al ser necesario disponer de permisos de administración como el usuario root. "adb" no puede ejecutar como root en versiones del sistema operativo Android de producción (con un tipo de "build" igual a "*user*"), es decir, en dispositivos móviles reales y no emuladores, salvo en dispositivos Android *rooted*:

```
$ getprop ro.build.type
getprop ro.build.type
user
```

501. En algunas versiones no oficiales de Android, como la versión *rooted* CyanogenMod[57] (CM), es posible modificar de forma permanente el nombre del dispositivo móvil a través del menú "Ajustes - Aplicaciones - Desarrollo - Nombre del dispositivo" (ejemplo correspondiente a la versión CM 7).

502. Las referencias internas a nombres empleadas por el dispositivo móvil Android por defecto pueden ser obtenidas a través de la utilidad "adb" y sus capacidades de depuración de las propiedades del dispositivo móvil ("adb shell getprop"):

[56] https://play.google.com/store/apps/details?id=nk.bla.android.autostart
[57] http://www.cyanogenmod.org



503. En caso de desvelarse el nombre del dispositivo en sus comunicaciones, como por ejemplo en el tráfico DHCP (donde se desvela el valor de la propiedad "net.hostname"; ver apartado "5.17.2. Seguridad en TCP/IP"), éste podría revelar detalles tanto del fabricante del dispositivo móvil, como por ejemplo el modelo del terminal, como del propietario. Estos datos serían muy útiles para un potencial atacante interesado en explotar vulnerabilidades en ese tipo concreto de dispositivo móvil o interesado en realizar ataques dirigidos hacia una persona concreta.

504. Adicionalmente, Android puede emplear otros nombres para el dispositivo móvil al hacer uso de diferentes servicios y tecnologías, como por ejemplo Bluetooth (ver apartado "5.13. Comunicaciones Bluetooth") o el punto de acceso Wi-Fi (ver apartado "5.14.6. Punto de acceso o zona Wi-Fi"), por lo que la configuración de los ajustes de Bluetooth o del punto de acceso Wi-Fi permiten modificar su valor.

Nota: el valor de la propiedad denominada "net.bt.name", con el valor "Android" por defecto, no está relacionada con el nombre Bluetooth del dispositivo móvil.

505. De ser posible en versiones futuras de Android, se recomienda modificar el nombre del dispositivo móvil por uno que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociada al mismo), como por ejemplo "dm0001" ("dispositivo móvil 0001").

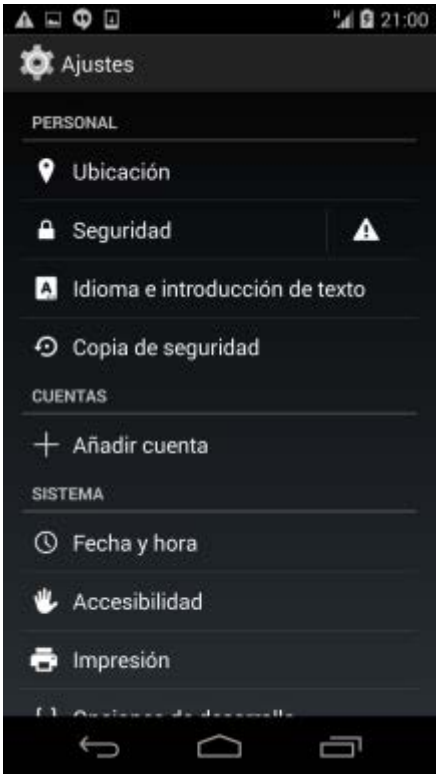
5.10 LOCALIZACIÓN (O UBICACIÓN) GEOGRÁFICA

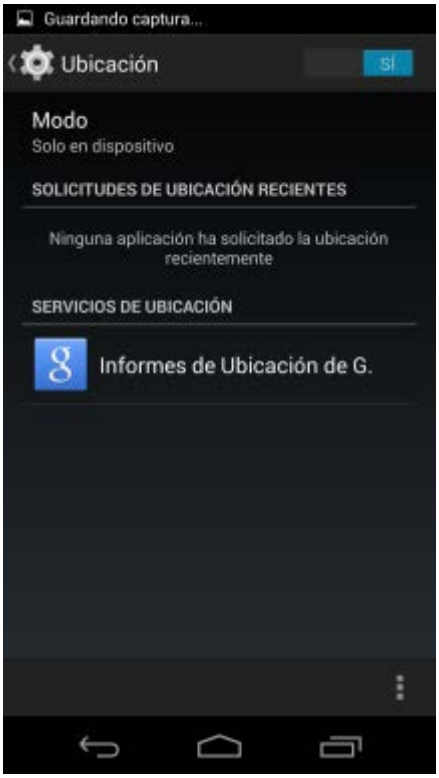
506. Las capacidades de localización (o ubicación) del dispositivo móvil a través del módulo de GPS, o de las redes de datos (telefonía móvil y Wi-Fi), pueden ser activadas y desactivadas por el usuario en función de su utilización.

507. El uso del GPS, o de los servicios de localización, en el dispositivo móvil Android viene reflejado por un conjunto específico de iconos mostrados a través de la barra superior de estado.

Nota: el dispositivo o módulo GPS en Android está activo únicamente cuando se está haciendo uso de una app con capacidades de localización, es decir, que hace uso del GPS, y en base a la configuración específica (modos), de los servicios de localización de Android.

508. Desde el menú "Ajustes [Personal] - Ubicación", y en concreto a través del botón "[SI | NO]" disponible en la parte superior derecha, es posible habilitar las capacidades de localización del dispositivo móvil:





509. Android 4.4 (KitKat) proporciona un mayor control sobre los diferentes modos de localización (o ubicación) disponibles [Ref.- 147]: alta precisión, ahorro de batería o solo en dispositivo.

510. La opción o el modo "Alta precisión" hace uso del módulo GPS, de las redes Wi-Fi y de telefonía móvil, y de otros sensores, para obtener la ubicación más rápida y precisa del dispositivo móvil. El modo "Ahorro de batería" emplea como fuentes para la obtención de la ubicación del dispositivo móvil las redes Wi-Fi y de telefonía móvil, ya que llevan a

cabo un menor consumo de energía en comparación al módulo GPS. Por último, el modo "Solo en dispositivo" hace uso únicamente del módulo GPS del dispositivo móvil.

511. La nueva funcionalidad y API empleada por las apps para acceder a los servicios de localización, especialmente al usar el modo "Ahorro de batería", reduce drásticamente el consumo de batería. Previamente, cada app que necesitaba hacer uso de los servicios de localización despertaba al módulo GPS hardware y obtenía su información de ubicación propia individualmente.

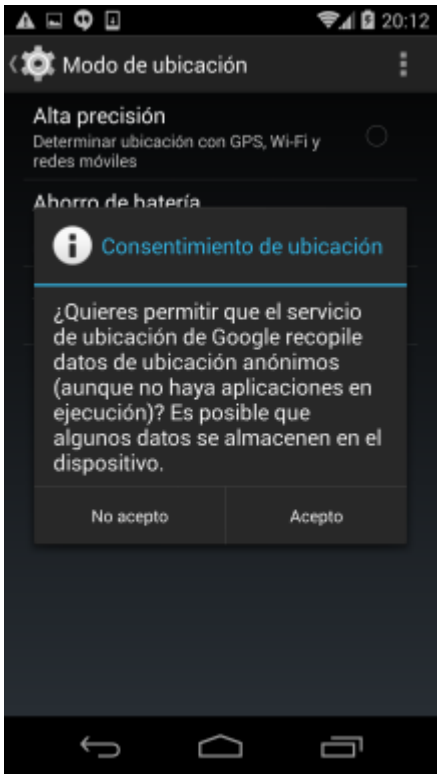
512. Todos estos modos están disponibles en los servicios de ubicación de Google, que extienden las capacidades del módulo GPS del dispositivo móvil con otras tecnologías.

513. La opción (o modo) habilitada por defecto dependerá de las opciones seleccionadas en la pantalla de "Ubicación y Google" durante el proceso inicial de instalación y configuración del dispositivo móvil (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial").

514. Debe tenerse en cuenta que el modo avión de Android deshabilitará los servicios de ubicación, no permitiendo ninguna transmisión inalámbrica ni con los satélites GPS, ni con las redes Wi-Fi o de telefonía móvil.

515. Desde el punto de vista de seguridad, si se desea que no se genere ningún tráfico desde el dispositivo móvil hacia los servicios de Google, se recomienda seleccionar la opción o modo "Solo en dispositivo", pese a que tenga asociado un mayor consumo de batería y tarde más tiempo en localizar la ubicación del dispositivo inicialmente.

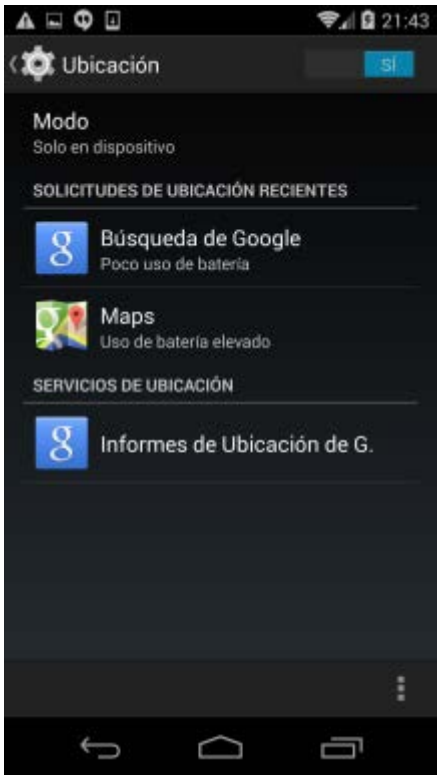
516. En el caso de habilitar las capacidades de localización a través de redes inalámbricas (Wi-Fi y telefonía móvil), mediante la selección de los modos "Alta precisión" o "Ahorro de batería" , Android solicita confirmación por parte del usuario para recopilar los datos de las señales inalámbricas recibidas y la ubicación del terminal de forma anónima:



Nota: existen estudios pasados que reflejan que la información de localización intercambiada entre el dispositivo móvil Android y Google no es completamente anónima, ya que aparte de incluir detalles de las señales de las redes inalámbricas recibidas y la ubicación del terminal, se incluye un identificador único del dispositivo móvil [Ref.- 79], afectando a la privacidad del usuario.

Adicionalmente, la información de las redes Wi-Fi recopilada por Google a través de los coches del programa StreetView y de los dispositivos móviles Android estuvo disponible en el pasado para su consulta a través de la API de Google y de páginas web externas [Ref.- 80], siendo posible conocer la ubicación de una red Wi-Fi a nivel mundial en base a su dirección MAC o BSSID. El acceso a través de este servicio no está disponible actualmente públicamente.

517. Es posible consultar las apps que han solicitado información sobre la ubicación del dispositivo móvil recientemente a través del menú "Ajustes [Personal] - Ubicación", y de la sección "Solicitudes de Ubicación Recientes":



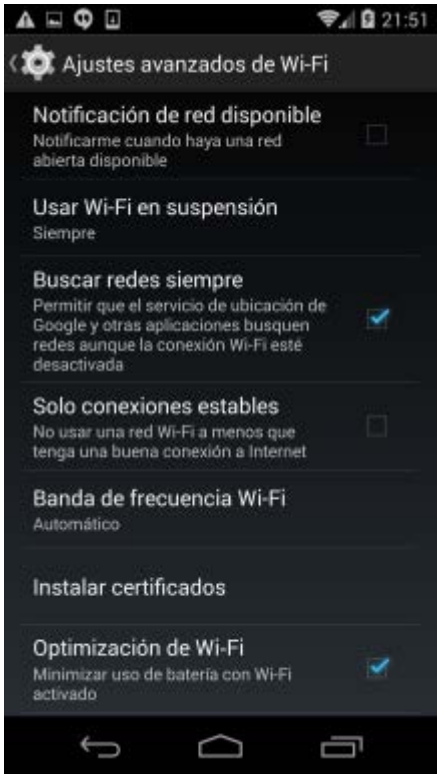
518. Mediante la visualización de las apps en la lista, bajo su nombre, es posible identificar el impacto en la batería debido al uso de los servicios de ubicación por parte de cada app: "Uso de batería elevado" o "Poco uso de batería".

519. Mediante la selección de una app de la lista se accede a la información de la app (información también disponible desde el menú "Ajustes [Dispositivo] - Aplicaciones - Todas").

520. Adicionalmente, una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil, a través del menú "Ajustes [Personal] - Ubicación", y de la sección "Servicios de Ubicación", es posible seleccionar "Informes de Ubicación de G." (Google) y acceder a los ajustes de configuración para activar o desactivar los informes de ubicación y el historial de ubicaciones de la cuenta de usuario de Google (ver apartado "5.10.5. Historial de ubicaciones e informes de ubicación"):

521. Adicionalmente, si se hace uso de alguno de los modos que emplean las redes Wi-Fi para obtener información sobre la ubicación del dispositivo móvil, es posible configurar si se permite el uso de las capacidades Wi-Fi del dispositivo móvil para estos servicios y, en concreto, para la búsqueda e identificación de redes Wi-Fi, aunque la conexión o el interfaz Wi-Fi esté desactivado.

522. Esta opción de configuración también está disponible en el proceso de instalación y configuración inicial del terminal, ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial"), y se puede acceder a la misma posteriormente desde el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre":



523. Por último, la activación de los servicios de ubicación en el dispositivo móvil también está disponible a través de los ajustes rápidos, accesibles desde la barra superior de estado.

524. Se recomienda deshabilitar las capacidades de localización del dispositivo móvil salvo que se esté haciendo uso explícito de esta funcionalidad. En caso de habilitar dichas capacidades, se recomienda activar únicamente la localización mediante GPS, no haciendo uso de las capacidades de localización mediante redes Wi-Fi o redes de telefonía móvil.

5.10.1 SERVICIOS DE UBICACIÓN DE GOOGLE

525. Durante el proceso de configuración inicial asociado al dispositivo móvil empleado para la elaboración de la presente guía, incluso aunque se omita la asociación del dispositivo a una cuenta de usuario de Google, Android solicita al usuario si desea usar los servicios de ubicación de Google. Las dos opciones disponibles ("Permitir que el servicio de ubicación de Google recopile datos de ubicación anónimos…" y "Utilizar Mi ubicación para los resultados de búsqueda de Google y otros servicios…") están habilitadas por defecto.

526. Se recomienda deshabilitar ambas opciones durante el proceso inicial de instalación y configuración del dispositivo móvil (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial").

527. Los servicios de ubicación o localización de Google (*Google Location Services*), permiten a las apps conocer la ubicación geográfica aproximada del dispositivo móvil, y por tanto del usuario, sin disponer de señal GPS, y hacer uso de esa información en los servicios de búsqueda (y otros) de Google, o desde cualquier app con los permisos adecuados, teóricamente de una forma más rápida y precisa.

528. La ubicación se obtiene a través de la información de localización disponible sobre torres (o redes) de telefonía móvil y redes Wi-Fi, y la señal recibida en cada momento por el dispositivo móvil para ambas tecnologías (telefonía móvil y Wi-Fi), en lugar de emplear información más precisa como la proporcionada por el dispositivo o módulo GPS.

529. La utilización de los servicios de ubicación de Google pueden conllevar por tanto el envío, supuestamente anónimo, a Google de los datos recopilados sobre las redes Wi-Fi y de telefonía móvil por parte del dispositivo móvil, incluso aunque no se esté utilizando ninguna app.

530. En resumen, estas peticiones de información hacia Google pueden desvelar información de las redes, Wi-Fi y de telefonía móvil existentes en el área de cobertura del dispositivo móvil, así como otros detalles relevantes del terminal, potencialmente[58] a cualquiera que esté capturando el tráfico de datos generado desde el dispositivo móvil. Las respuestas de los servicios de ubicación de Google, en formato binario, contienen información de la ubicación estimada del dispositivo móvil.

531. Se recomienda limitar el uso de estos servicios, por parte de cualquier app como por ejemplo "Google Maps" (ver siguiente apartado), y específicamente su utilización cuando se emplea algo más que el módulo GPS, ya que los servicios de ubicación de Google a través de torres de telefonía móvil y redes Wi-Fi desvelan detalles privados del dispositivo móvil y su ubicación.

5.10.2 GOOGLE MAPS

532. Los servicios de ubicación de Google son utilizados, entre otros, tanto por el propio sistema operativo Android, como por las apps disponibles por defecto o proporcionadas por terceros, como por ejemplo la app "Maps" o "Google Maps" (for Android; http://m.google.com/maps), que en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como app por defecto a través de la app "Maps" (disponible desde el *Launcher*).

Nota: la app Google Maps ("Maps") requiere disponer de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información cartográfica de los mapas.

533. Tras aceptar los términos y condiciones del servicio (al ejecutar la app la primera vez), y en función de la configuración de los servicios de ubicación, la recopilación de información (de redes Wi-Fi y torres de telefonía) será activada y se permitirá su utilización por defecto por parte de las apps que hacen uso de los servicios de ubicación.

534. En caso de no haber configurado el modo de "Alta precisión" de los servicios de ubicación, se mostrará un mensaje sugiriendo su activación:

[58] Versiones pasadas de los servicios de localización de Google enviaban tráfico no cifrado mediante HTTP.

535. Desde "Maps" es posible hacer uso de la información de localización, en concreto, empleando el botón circular con una cruceta, que centrará el mapa en la localización actual del usuario (identificada por una indicador azul); ver imagen superior derecha.

536. Al hacer uso de apps que requieren conocer la ubicación del usuario, como "Maps", si han sido habilitadas se emplearán las capacidades para localizar la ubicación del dispositivo móvil incluso cuando no se dispone de módulo GPS (o éste no está activo o no hay cobertura de los satélites GPS), a través de A-GPS, que emplea la información de localización disponible a través de servicios de terceros (ver apartado "5.10.3. A-GPS"), y la funcionalidad extendida de los servicios de ubicación de Google descritos previamente, haciendo uso de la información de las redes Wi-Fi y las torres de telefonía móvil.

537. Los servicios de ubicación de Google integrados en Google Maps, así como los datos e información obtenida por la app (mapas, información extra, etc), en el caso de la versión 7.5.0 de la app "Maps" disponible por defecto en Android 4.4.4, emplean únicamente conexiones mediante HTTPS (cifradas) desde el dispositivo móvil hacia múltiples servidores de Google.

538. Este cambio en el funcionamiento respecto al comportamiento de versiones previas de la app y versiones previas de Android evita que un potencial atacante acceda al tráfico de red y pueda obtener detalles de la ubicación de usuario y de las redes inalámbricas (como por ejemplo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía móvil (como por ejemplo el identificador de torre, y los códigos de área (LAC), operador de telefonía móvil (MNC) y país (MCC)) existentes en el área de cobertura del dispositivo móvil.

5.10.3 A-GPS

539. *Assisted GPS* (A-GPS o aGPS) es un sistema de ayuda para mejorar la obtención de información y la precisión de los datos de localización obtenidos mediante GPS, que permite disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.

540. Especialmente A-GPS permite agilizar significativamente el tiempo necesario para ubicar inicialmente el dispositivo móvil, parámetro conocido como TTFF (Time-To-First-Fix).

541. El módulo A-GPS está (teóricamente) disponible en dispositivos móviles Android con GPS, especialmente cuando se hace uso del modo de alta precisión.

542. El sistema A-GPS es un sistema híbrido que se basa en obtener información de las torres de telefonía móvil detectadas desde la ubicación del dispositivo móvil (y que proporcionan información auxiliar o de asistencia sobre la ubicación), y adicionalmente, hace uso de las conexiones de datos (habitualmente 2/3/4G, o Wi-Fi) del dispositivo móvil para obtener información actualizada de dónde se encuentran los diferentes satélites GPS en un momento temporal (información con datos de las órbitas y de sincronización - reloj - de los satélites, conocido también como almanaque).

543. Por tanto, la funcionalidad A-GPS también es visible a través del tráfico de datos del dispositivo móvil. Android 4.x, en diferentes momentos temporales como por ejemplo durante el proceso de arranque del dispositivo móvil, envía tráfico no cifrado hacia los servidores de gpsOneXTRA (ver apartado "5.10.4. gpsOneXTRA").

544. Debe tenerse en cuenta que pese a que el uso del módulo GPS está siempre habilitado por defecto si los servicios de ubicación están activos, salvo que se haga uso del modo de ahorro de batería, hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que las apps como "Maps" harán uso automáticamente de las capacidades de ubicación sin hacer uso del módulo GPS si estás han sido habilitadas, por ejemplo, en el modo de alta precisión.

545. En resumen, se recomienda deshabilitar la funcionalidad A-GPS mediante la activación del modo "Solo en dispositivo" salvo que se quiera hacer uso explícito de estas capacidades, con el objetivo de evitar desvelar información de la ubicación del dispositivo móvil (por ejemplo, torres de telefonía móvil o redes Wi-Fi cercanas) a través del tráfico de datos cifrado destinado a los servidores de Google.

5.10.4 GPSONEXTRA

546. Con el objetivo de agilizar el proceso de localización, complementando las coordenadas obtenidas del módulo GPS y su precisión, los dispositivos móviles Android pueden disponer de la funcionalidad asociada a la asistencia mediante gpsOneXTRA (aplicación conocida como QuickGPS en otras plataformas móviles).

547. Esta funcionalidad se conecta a un servidor web de "gpsonextra.net" (xtra1, xtra2 ó xtra3) para descargar la información semanal de la localización de los satélites GPS alrededor del planeta. Por defecto, la descarga automática de esta información está habilitada.

548. La descarga se lleva a cabo mediante el protocolo HTTP (TCP/80), sin cifrar, hacia los servidores de "gpsonextra.net" mencionados previamente, descargándose el fichero "/xtra2.bin". Para ello, Android emplea el siguiente agente de usuario que permite identificar el tipo de cliente: "User-Agent: Android".

549. Adicionalmente Android 4.x incluye en la petición otras cabeceras HTTP que desvelan detalles del dispositivo móvil:

```
GET /xtra2.bin HTTP/1.1
Accept: */*, application/vnd.wap.mms-message, application/vnd.wap.sic
x-wap-profile:
    http://www.openmobilealliance.org/tech/profiles/UAPROF/ccppschema-
    20021212#
Host: xtra3.gpsonextra.net
Connection: Keep-Alive
User-Agent: Android
```

Nota: la configuración interna de Android tanto del servidor de tiempos NTP (ver apartado "5.17.2. Seguridad en TCP/IP"), como de los servidores de gpsOneXTRA y A-GPS (ver apartado "5.10.3. A-GPS") está disponible en el fichero "/system/etc/gps.conf", aunque no se dispone de ningún ajuste de configuración a través del interfaz gráfico de usuario de Android para modificar estos parámetros. Ejemplo (parcial) del fichero "gps.conf":

```
XTRA_SERVER_1=http://xtra1.gpsonextra.net/xtra2.bin
XTRA_SERVER_2=http://xtra2.gpsonextra.net/xtra2.bin
XTRA_SERVER_3=http://xtra3.gpsonextra.net/xtra2.bin
NTP_SERVER=time.gpsonextra.net[59]
SUPL_HOST=supl.google.com
SUPL_PORT=7275
```

550. Las conexiones NTP (UDP/123), para la sincronización horaria, y gpsOneXTRA ("xtraN.gpsonextra.net", TCP/80), para incrementar la precisión de localización del GPS, se llevan a cabo (por ejemplo) cada vez que se enciende el dispositivo móvil y éste dispone de acceso a Internet.

551. Si no se desea que el dispositivo móvil realice las conexiones NTP, gpsOneXTRA y A-GPS indicadas, por motivos de seguridad y para limitar las conexiones de datos y la posible información revelada a través de éstas, será necesario modificar el fichero "gps.conf" a través del interfaz de depuración de Android desde un ordenador a través del puerto USB, empleando la utilidad ADB. Este fichero de configuración sólo puede ser modificado en dispositivos móviles Android *rooted*, ya que sólo el usuario root dispone de permisos de escritura bajo el sistema de ficheros "/system" (qué está montado por defecto sólo con permisos de lectura, "ro"):

```
C:\> adb shell

$ mount | grep system
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4 ro,seclabel,
relatime,data=ordered 0 0

$ cd /system/etc
$ mv gps.conf gps.conf.bak
failed on 'gps.conf' - Read-only file system
$
```

552. La funcionalidad de dichos protocolos se verá afectada en caso de ser deshabilitados.

[59] Se han identificado peticiones NTP también hacia el servidor "x.ns.gin.ntt.net".

5.10.5 HISTORIAL DE UBICACIONES E INFORMES DE UBICACIÓN

553. Los servicios de Google pueden hacer uso de los datos del historial de ubicaciones, obtenidos a través de los informes de ubicación, para por ejemplo, mejorar los resultados de búsqueda de Google Maps (mediante la app "Maps") en función de los sitios frecuentados habitualmente por el usuario [Ref.- 164].

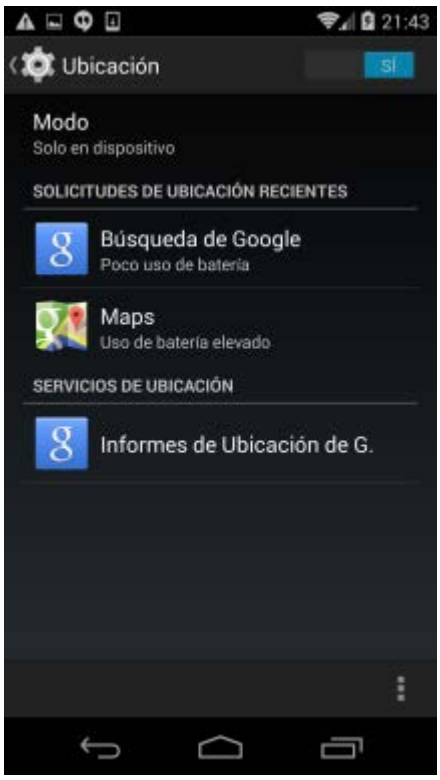
554. El historial de ubicaciones almacena un registro histórico de la ubicación del usuario procedente de todos los dispositivos móviles en los que el usuario haya iniciado sesión con su cuenta de usuario de Google. Para que se envíe la información al historial, y se pueda almacenar, el dispositivo móvil debe tener habilitados los informes de ubicación.

555. Los informes de ubicación permiten a Google utilizar (y potencialmente almacenar) periódicamente los datos de ubicación más recientes del dispositivo móvil, así como la información sobre las actividades que conllevan movimiento (conducir, caminar, pasear en bicicleta, etc) y asociarlos a la cuenta de usuario de Google.

556. La frecuencia con la que los informes de ubicación actualizan los datos de ubicación no es fija y depende de diferentes factores, como la batería del dispositivo móvil, si el usuario se está desplazando, o la velocidad a la que se desplaza.

557. Los informes de ubicación (como la configuración del historial de ubicaciones directamente desde el dispositivo móvil) están disponibles en dispositivos móviles con Android 2.3 (o versiones superiores) que tengan instalada la versión 6.14.5 (o una versión superior) de la app "Maps". La versión de esta app disponible por defecto en Android 4.4.4 es la 7.5.0.

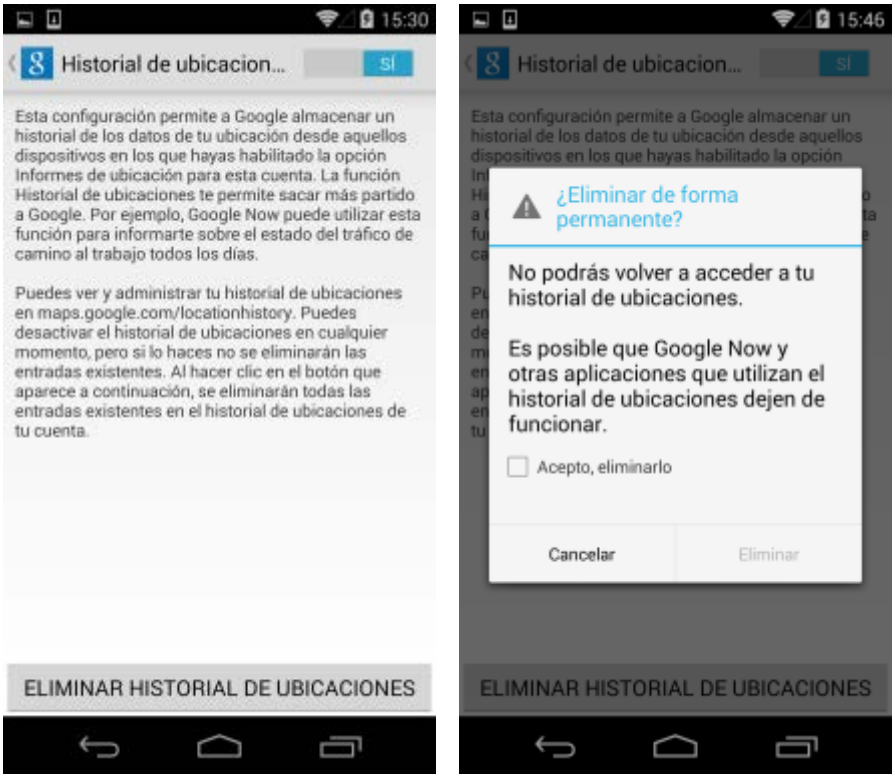
558. A través del menú "Ajustes [Personal] - Ubicación", y de la sección "Servicios de Ubicación", es posible seleccionar "Informes de Ubicación de G." (Google) y acceder a los ajustes de configuración para activar o desactivar los informes de ubicación y el historial de ubicaciones de la cuenta de usuario de Google:



559. Al activar los informes de ubicación, también se permite el envío de información de uso y diagnóstico a Google sobre el funcionamiento de los informes de ubicación [Ref.- 164], incluyendo información detallada sobre las diferentes actividades del terminal y del usuario.

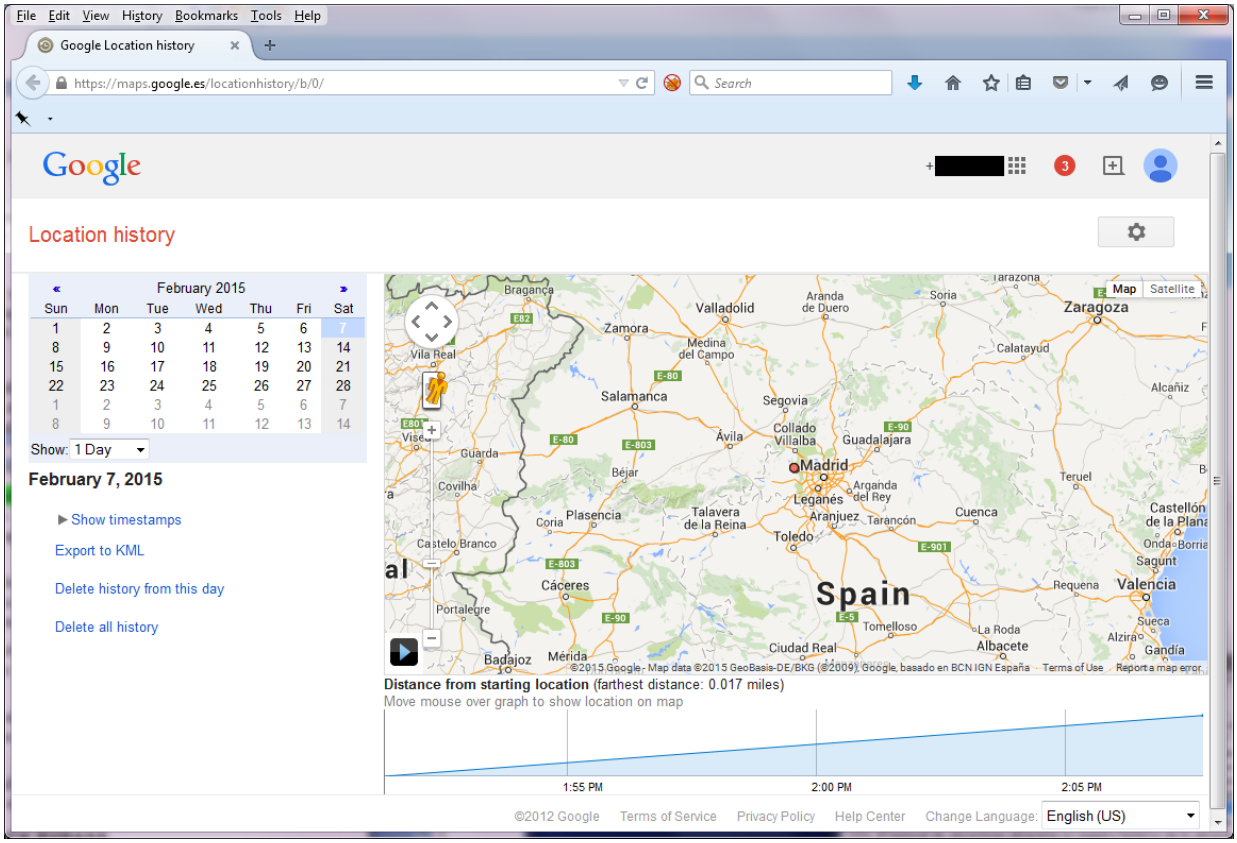
560. En primer lugar, la configuración de los informes de ubicación está disponible a través del menú mencionado previamente, y la opción "Informes de ubicación" (puede (des)activarse mediante el botón "[SI | NO]"):

561. Por otro lado, la configuración del historial de ubicaciones está disponible a través del menú mencionado previamente, y la opción "Historial de ubicaciones" (puede (des)activarse mediante el botón "[SI | NO]"). La pantalla asociada dispone del botón "Eliminar Historial de Ubicaciones" en su parte inferior para borrar los datos de ubicaciones previamente almacenados por Google:

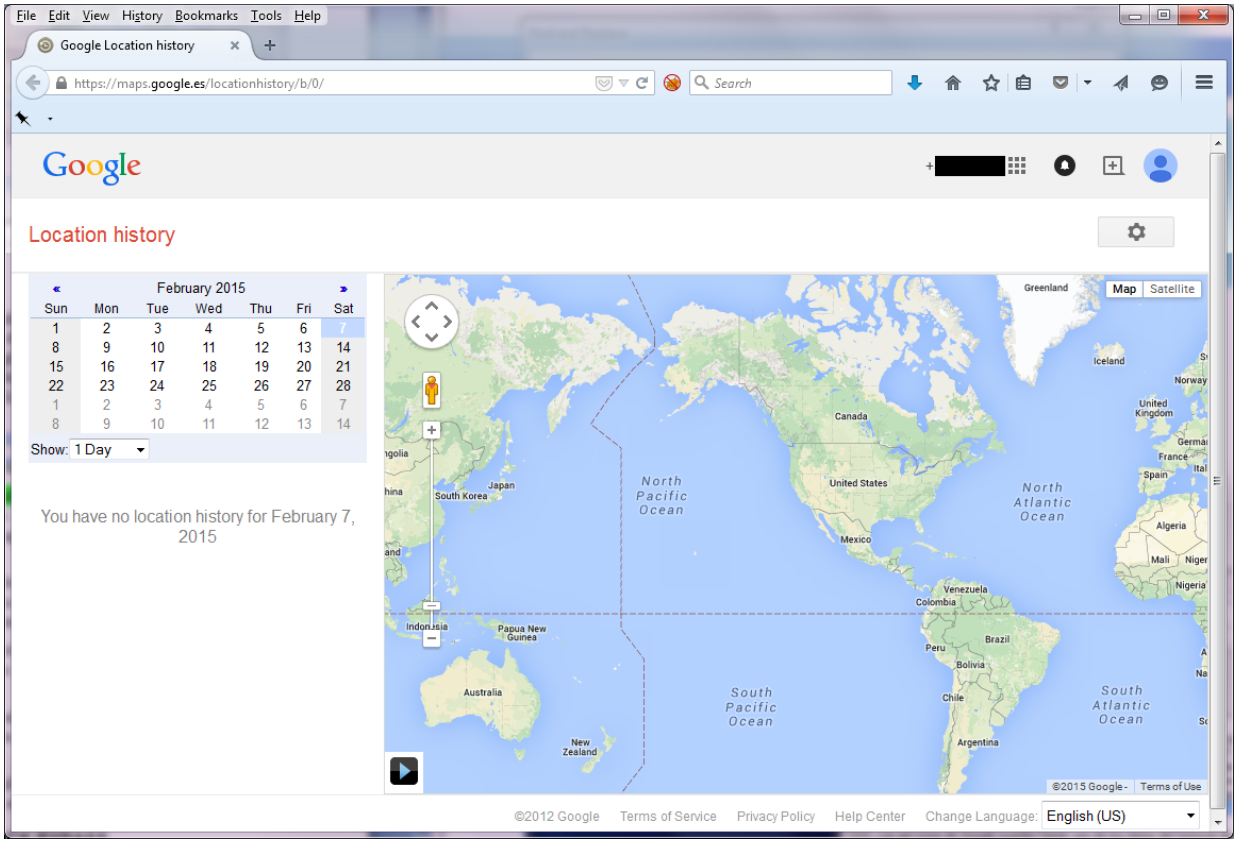


562. Finalmente, un usuario puede también acceder y administrar el historial de ubicaciones vinculado a su cuenta de usuario de Google a través de la siguiente URL: "https://maps.google.com/locationhistory/". Esta funcionalidad está asociada al "Historial de la cuenta", disponible desde "https://www.google.com/settings/accounthistory" (y que también permite el acceso al historial de actividad web y de aplicaciones, ver apartado "5.22.1.5. Historial de actividad web y de aplicaciones").

563. Desde la misma es posible obtener los detalles de las ubicaciones registradas para el usuario, incluso clasificadas por fechas y horas, y obtener información de distancias entre ubicaciones:



564. Desde la página web es posible eliminar los registros del historial para una fecha concreta, o todo el historial. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:



565. En resumen, desde el punto de vista de seguridad, y de la privacidad el usuario, no se recomienda hacer uso de los informes de ubicación (es decir, enviar ese tipo de datos de ubicación a Google), ni del historial de ubicaciones (es decir, permitir a Google que almacene un histórico de los datos de ubicación). Adicionalmente, se recomienda borrar el historial de ubicaciones actualmente existente en la cuenta de usuario de Google.

5.10.6 OTRAS APPS QUE HACEN USO DE LA LOCALIZACIÓN

Nota: queda fuera del alcance de la presente guía realizar un análisis detallado de seguridad de las diferentes apps que hacen uso de los servicios de localización de Google en Android, así como de la existencia de posibles vulnerabilidades en las mismas. A continuación se muestran ejemplos de algunas apps, incidiendo únicamente en si hacen uso de tráfico cifrado mediante HTTPS, o si exponen los datos intercambiados entre ellas y los servidores remotos mediante tráfico no cifrado, normalmente empleando el protocolo HTTP. A modo de ejemplo se menciona únicamente el valor del agente de usuario (o "User-Agent") desvelado por las apps, que proporciona numerosos detalles sobre la app y el dispositivo móvil asociado.

Se recomienda no hacer uso de este tipo de apps o servicios que desvelan información detallada de la ubicación del usuario y del dispositivo móvil empleado, y que hacen uso de conexiones HTTP no cifradas, salvo que explícitamente se deseé acceder a la información que éstos proporcionan.

La mayoría de apps mencionadas requieren de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información necesaria para su funcionalidad.

5.10.6.1 GOOGLE MAPS: NAVEGACIÓN

566. Las capacidades de localización también pueden ser empleadas por otras apps, o por funcionalidades adicionales de apps existentes, como por ejemplo las capacidades de navegación de la app "Maps"[60], que en Android 4.4.4 están integradas dentro de dicha app (y hacen uso de HTTPS).

5.10.6.2 GOOGLE EARTH

567. Otras apps o servicios de Google disponibles por defecto en Android, como por ejemplo "Google Earth" a través de la app "Earth", también hacen uso de las capacidades de localización de Android.

568. La app no cifra su tráfico mediante HTTPS, sino que hace uso de tráfico no cifrado mediante HTTP, desvelando entre otros su agente de usuario:

```
User-Agent: GoogleEarth/7.1.0003.1255(Android;Android (Nexus 5-
hammerhead-user-4.4.4);es-ES;kml:2.2;client:Free;type:default)
```

5.10.6.3 GOGGLES

569. Las capacidades de localización también pueden ser empleadas por otras apps como Goggles (http://www.google.com/mobile/goggles/), que permite la búsqueda de imágenes a través de fotos y que está disponible como app a través de Google Play.

[60] http://www.google.com/mobile/maps/

570. Goggles es una aplicación de realidad aumentada que permite realizar búsquedas en Google mediante fotografías en lugar de emplear términos de búsqueda. Para ello el usuario únicamente debe tomar una fotografía de algo que esté viendo o en lo que esté interesado, y emplear dicha fotografía para encontrar más información sobre su contenido (como por ejemplo cosas, lugares o negocios) a través de Google.

571. Googles puede ser empleada para obtener información de lugares y negocios cercanos al que nos encontramos en un momento determinado. Para ello hace uso de la información de localización del GPS del dispositivo móvil.

5.10.6.4 NOTICIAS Y TIEMPO

572. La app "Noticias y tiempo", que proporciona noticias informativas e información meteorológica (tiempo), disponible también como *widget* y dentro de los servicios de Google Now, hace uso de las capacidades de localización de Android:

573. La app no cifra su tráfico mediante HTTPS, sino que hace uso de tráfico no cifrado mediante HTTP, desvelando entre otros diferentes agentes de usuario:

```
User-Agent: GoogleMobile/1.0 (hammerhead KTU84P); gzip
User-Agent: Dalvik/2.0.0 (Linux; U; Android 4.4.4; Nexus 5 Build/KTU84P)
```

5.10.6.5 BUSCADOR DE GOOGLE

574. La información de los servicios de localización puede ser empleada por otros servicios o apps de Google, como por ejemplo el buscador web.

575. Es posible habilitar la funcionalidad de localización directamente desde Google (el buscador de Google, disponible en "www.google.com" o en sus variantes localizadas en

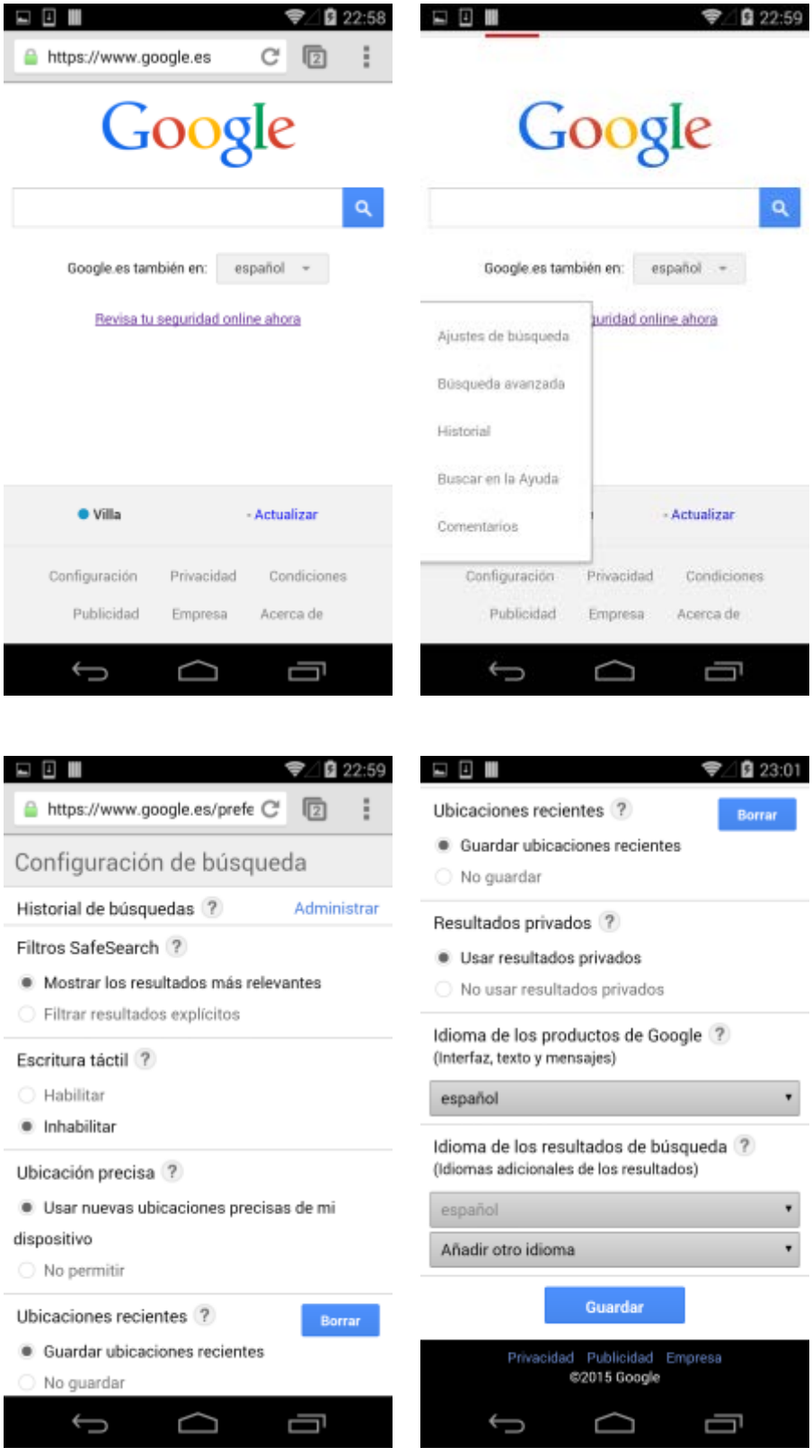
cada país[61]) empleando el navegador web desde el dispositivo móvil Android ("Chrome"). Al acceder al buscador se solicita al usuario utilizar la ubicación del dispositivo móvil, pudiendo permitir o denegar dicho acceso:

576. Si se permite el acceso, se mostrará en la parte inferior la ubicación del usuario. Es decir, el acceso a la página web principal del buscador de Google solicitará autorización al usuario para compartir su ubicación, y reflejará si se está haciendo uso de la ubicación del dispositivo móvil o no, y cuál es la ubicación actual empleada.

577. Los permisos habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente (ver apartado "5.10.6.7. Navegador web").

578. Por otro lado, a través de la opción "Configuración" disponible en la parte inferior de la página web principal de "www.google.com", a través de la opción "Ajustes de búsqueda", se puede habilitar el parámetro "Ubicación precisa" (habilitada por defecto), pudiendo seleccionar "No permitir" el acceso a la ubicación o "Usar nuevas ubicaciones precisas de mi dispositivo". Para almacenar los cambios en la configuración que es necesario guardar la nueva configuración mediante el botón "Guardar" situado en la parte inferior de la página web:

[61] Por simplificar, las referencias a Google indican "www.google.com" aunque en realidad se haga uso de la versión localizada para España, "www.google.es".



579. Por otro lado, la opción "Ubicaciones recientes" permite "No guardar" o "Guardar las ubicaciones recientes" (opción habilitada por defecto), así como eliminar mediante el botón "Borrar" las ubicaciones recientes guardadas (ver imagen superior derecha).

580. Si se va a hacer uso de la funcionalidad de búsqueda considerando la ubicación de manera puntual, se recomienda únicamente activar la funcionalidad, llevar a cabo la búsqueda y

volverla a desactivar. Se recomienda hacer un uso limitado de esta funcionalidad con el objetivo de proteger la privacidad del usuario.

581. El agente de usuario empleado por el navegador web de Android desvela los detalles de la plataforma, versión y modelo de dispositivo móvil (ver apartado "5.22.1. Navegación web: Navegador").

582. Todos los accesos web al buscador de Google se realizan actualmente empleando cifrado mediante HTTPS.

5.10.6.6 REDES SOCIALES

583. La información de localización puede integrarse también con las apps de acceso a redes sociales (y Web 2.0), siendo posible la publicación de la ubicación del usuario a través, por ejemplo, de Twitter o Facebook.

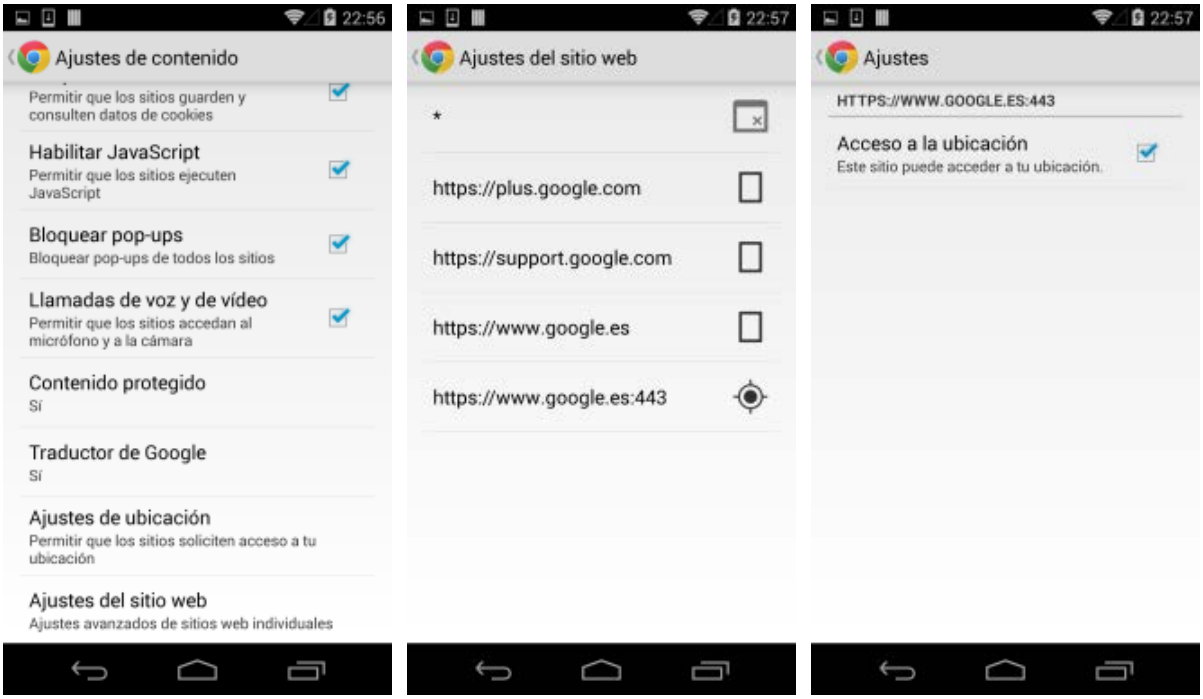
584. Debido a que las apps asociadas a estas redes sociales no están disponibles por defecto en Android 4.x, no se profundizará en los detalles centrados en deshabilitar el uso de los servicios de localización desde las mismas.

585. Desde el punto de vista de seguridad, se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales o servicios avanzados similares con el objetivo de proteger su privacidad.

5.10.6.7 NAVEGADOR WEB

586. El navegador web existente por defecto en Android ("Chrome") permite autorizar el acceso a la información de localización (o ubicación del dispositivo móvil) a todas las páginas web, de forma general (a través de los ajustes generales de configuración de los servicios de ubicación de Android), o a páginas web individuales.

587. Los permisos de acceso a la ubicación habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente desde el menú de "Ajustes" de "Chrome", y en concreto a través de la opción "Ajustes [Avanzados] - Ajustes de contenido - Ajustes del sitio web". Android dispone de capacidades granulares para definir qué sitios web disponen de acceso a la información de localización. Tras seleccionar un sitio web concreto, se puede deshabilitar la opción "Acceso a la ubicación":



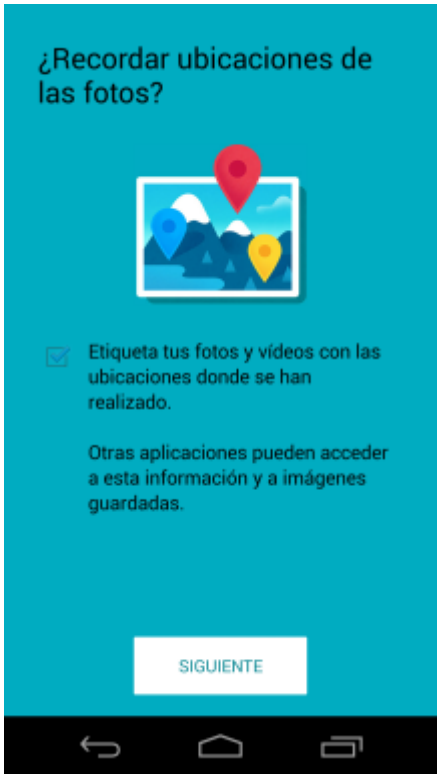
588. Los sitios web aparecerán en esta lista cuando han solicitado acceso a la ubicación y este acceso ha sido rechazado por el usuario (opción desactivada), o cuando ha sido permitido por el usuario, quedando reflejado en esta misma lista (opción activada).

589. Desde el punto de vista de seguridad se recomienda deshabilitar la opción "Acceso a la ubicación" para todos los sitios web, con el objetivo de no permitir a ningún sitio web disponer de acceso a la información de localización, incluso aunque tuvieran este acceso previamente permitido de forma individual.

5.10.7 INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

590. Android permite añadir información de la localización geográfica a las fotografías y vídeos realizados con la cámara del dispositivo móvil. Al realizar la fotografía (o vídeo) se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.

591. La primera vez que se ejecuta la app "Cámara" se pregunta al usuario si desea etiquetar las fotografías y vídeos con la información de la ubicación dónde se han realizado (opción habilitada por defecto), información también accesible para otras apps:



592. Desde el punto de vista de seguridad se recomienda deshabilitar esta funcionalidad con el objetivo de no desvelar detalles de las ubicaciones del usuario.

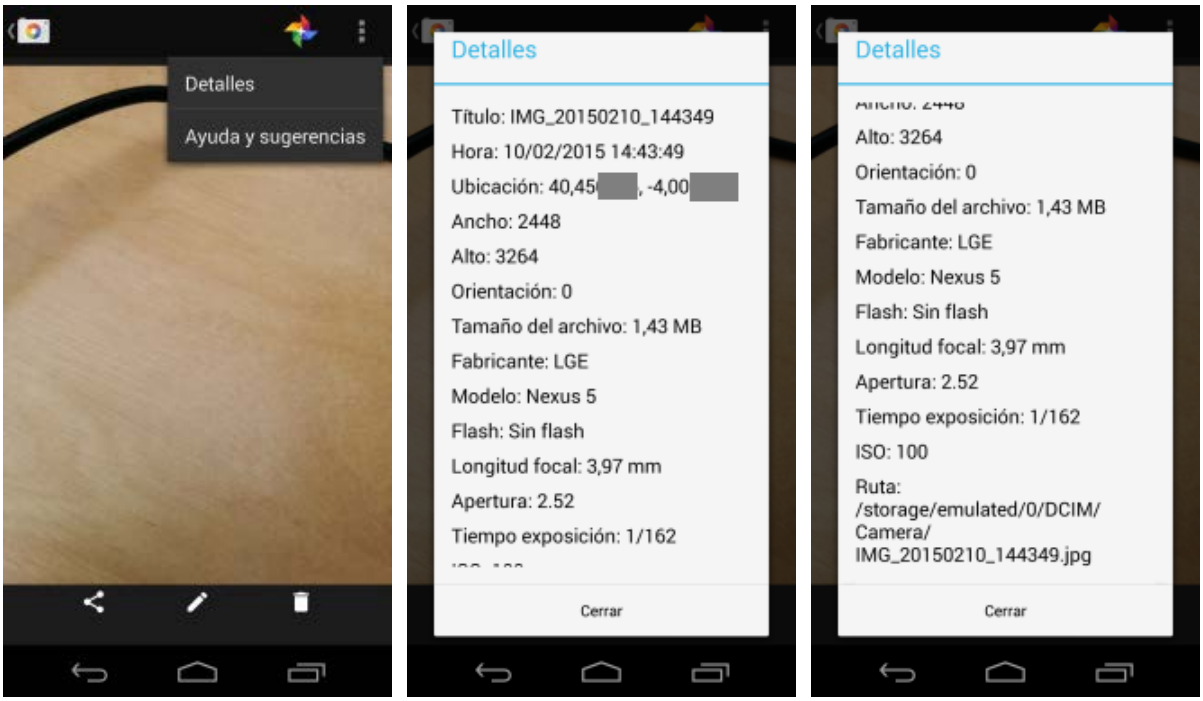
593. Esta funcionalidad puede ser habilitada y deshabilitada en cualquier momento a través del menú de configuración de la cámara. Para ello es necesario abrir la cámara mediante la app "Cámara" desde el *Launcher*, desplazar desde la izquierda hacia la derecha la imagen de la cámara, y seleccionar el botón de configuración de la parte inferior derecha:

594. La opción "Guardar ubicación" permite habilitar o deshabilitar esta funcionalidad.

595. Por defecto, las fotografías tomadas con el dispositivo móvil incluyen la información del GPS si no se modificaron las opciones de configuración iniciales de la app "Cámara".

596. Los detalles de ubicación de las fotografías pueden ser visualizados desde el dispositivo móvil Android, y en concreto, desde la galería de imágenes de la cámara. La galería está disponible tanto desde la app "Cámara", desplazando desde la derecha hacia la izquierda la imagen de la cámara, o también desde la app "Fotos" o desde la app "Galería" (ambas accesibles desde el *Launcher*).

597. Para ello es necesario emplear el botón de menú, y la opción "Detalles" (ejemplo asociado a la app "Cámara"):



598. El campo "Ubicación" (al comienzo de la lista de atributos de la imagen) indicará la ubicación dónde fue tomada (latitud y longitud). En caso de no disponer de la información de ubicación de la imagen, este campo o atributo no será mostrado.

599. Se recomienda no hacer uso de la funcionalidad que incluye la información del GPS en fotografías o vídeos, especialmente para su publicación o distribución en Internet, salvo que se quiera hacer uso explícito de estas capacidades. En caso contrario, las imágenes y vídeos revelarán los detalles exactos de dónde han sido tomadas.

5.11 COMUNICACIONES USB

600. La conexión USB del dispositivo móvil a un ordenador proporciona dos funcionalidades o tipos de conexiones diferentes: [Ref.- 91]

- Unidad de disco, para compartir la tarjeta de almacenamiento externa (en caso de disponer de una) y otras capacidades de almacenamiento internas del dispositivo móvil con el ordenador.
    - Los dispositivos móviles Android que no disponen de una tarjeta de almacenamiento externa física, simulan su existencia compartiendo parte de las capacidades de almacenamiento internas del dispositivo móvil.

- Conexión de telefonía móvil de datos, o *tethering*, para compartir la conexión de datos 2/3/4G o Wi-Fi del dispositivo móvil con el ordenador.
    - La compartición de la conexión a Internet a través de USB o Bluetooth puede hacer uso tanto de la conexión de datos 2/3/4G como de la conexión Wi-Fi del dispositivo móvil. La compartición a través de Wi-Fi (punto de acceso o zona Wi-Fi) sólo puede hacer uso de la conexión de datos 2/3/4G, ya que el interfaz Wi-Fi no puede actuar simultáneamente de cliente y de punto de acceso.

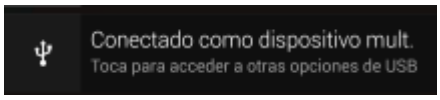
601. Ambas funcionalidades USB no pueden ser utilizadas simultáneamente. En caso de estar usando las capacidades de *tethering*, éstas deben ser deshabilitadas para tener acceso al almacenamiento vía USB, y viceversa.

5.11.1 ALMACENAMIENTO USB

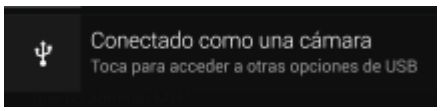
Nota: el acceso al dispositivo móvil como unidad de almacenamiento USB puede estar disponible incluso con el modo de depuración USB habilitado en Android. En caso de conflictos, si está habilitado, basta con deshabilitar este modo (opción recomendada desde el punto de vista de seguridad), para disponer de las capacidades de almacenamiento USB únicamente. El modo de depuración se puede deshabilitar mediante el menú "Ajustes [Sistema] - Opciones de desarrollo" (una vez habilitadas), desactivando la opción "Depuración USB".

602. Para acceder a las capacidades de almacenamiento USB basta con conectar el dispositivo móvil al ordenador mediante el puerto USB. Como resultado, se generará una notificación correspondiente en la barra superior de estado, "Conectado como ...", que puede tener dos estados:

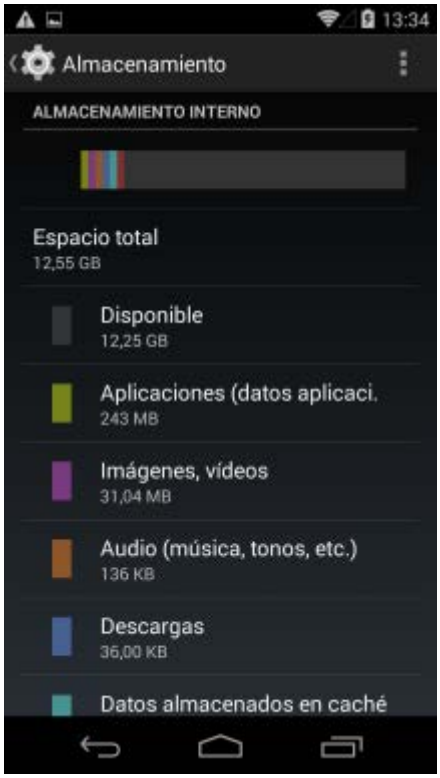
- "Conectado como dispositivo multimedia" (MTP, Media Transfer Protocol), dónde se simula un dispositivo multimedia que proporciona acceso a distintos tipos de ficheros a través de múltiples carpetas, incluyendo las de una cámara (descritas a continuación).



- "Conectado como una cámara" (PTP, Photo Transfer Protocol), dónde se simula una cámara de fotos (y/o vídeo) y se proporciona acceso únicamente a las fotos desde dos carpetas, "DCIM" y "Pictures".

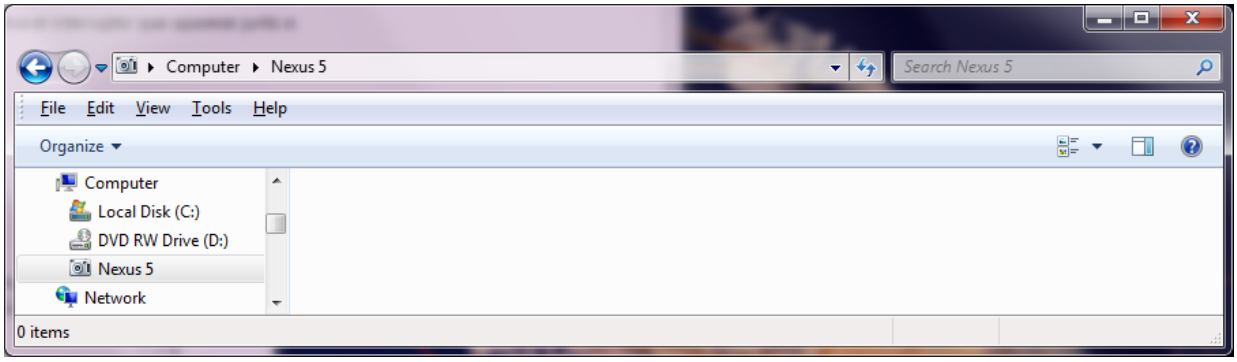


603. La implementación de las capacidades de almacenamiento externo en el dispositivo móvil empleado para la elaboración de la presente guía (específicas en función del modelo de dispositivo móvil basado en Android), al no disponer de una tarjeta de almacenamiento externa (o tarjeta SD) real (ver apartado "5.6.2. Cifrado de las tarjetas de almacenamiento externas"), no permiten acceder a esos contenidos como un sistema de almacenamiento masivo USB real (USB Mass Storage, UMS), no siendo por ejemplo posible asignar una letra de unidad en Windows a este espacio de almacenamiento. Sin embargo, esta limitación permite que tanto el dispositivo móvil como el ordenador puedan acceder simultáneamente al almacenamiento externo (virtual) del terminal:

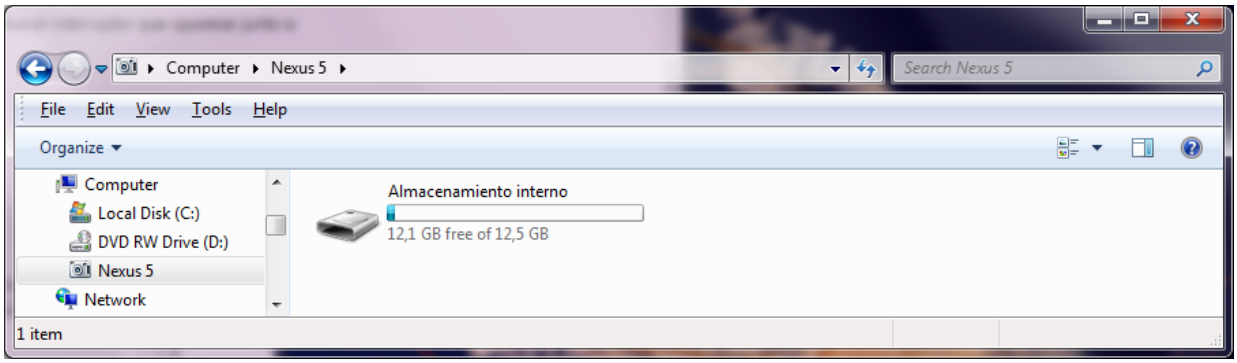


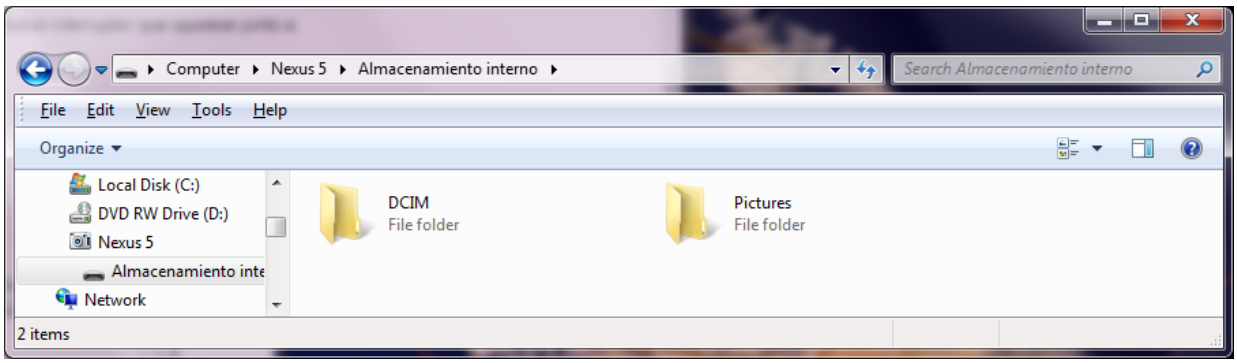
604. Es posible seleccionar los dos modos de conexión mediante la selección de la notificación, y la utilización de los botones correspondientes a ambos estados: "Dispositivo multimedia (MTP)" o "Cámara (PTP)". Estas opciones también están disponibles a través del menú "Ajustes [Dispositivo] - Almacenamiento - [...] - Conexión USB a ordenador":

605. Tras arrancar el dispositivo móvil, si se ha establecido un código de acceso y aún no ha sido introducido, la conexión USB desde el ordenador permite identificar la presencia del dispositivo, pero no se dispone de acceso a sus contenidos:



606. Para poder acceder a sus contenidos es necesario al menos haber desbloqueado una vez el dispositivo móvil desde su arranque. Una vez desbloqueado al menos en una ocasión, ya es posible disponer de acceso a sus contenidos en cualquier momento, incluso aunque el dispositivo móvil se encuentre de nuevo bloqueado:





607. La unidad de almacenamiento compartida con el ordenador corresponde a una sección denominada "Almacenamiento interno", ya que por ejemplo, el dispositivo móvil empleado para la elaboración de la presente guía no dispone de una tarjeta de almacenamiento externo (o tarjeta SD) física o real.

608. Debe prestarse especial atención a la configuración de seguridad del ordenador, y en concreto a los mecanismos de auto-ejecución de Windows (autorun y autoplay), para evitar la propagación de software malicioso (como por ejemplo el troyano Ambler u otros códigos dañinos, como en el caso de Vodafone y Android en 2010 [Ref.- 1]) desde la tarjeta de almacenamiento externa del dispositivo móvil compartida con el ordenador.

5.11.2 CONEXIÓN DE DE RED COMPARTIDA POR USB (*TETHERING*)

609. La opción de conexión compartida, o *tethering*, permite compartir la conexión de datos de telefonía móvil (2/3/4G) o Wi-Fi del terminal con un ordenador. Desde el punto de vista de

seguridad se recomienda hacer uso de *tethering* mediante cable USB, en lugar de mediante Bluetooth (en particular) o de Wi-Fi [Ref.- 91].

610. Las capacidades de *tethering* (tanto por USB como por Bluetooth, ver apartado "5.13.7. Conexión de red compartida por Bluetooth") y de punto de acceso Wi-Fi (ver apartado "5.14.6. Punto de acceso o zona Wi-Fi") pueden ser utilizadas simultáneamente en Android, proporcionando conexión de red a otros dispositivos u ordenadores simultáneamente tanto por USB, como por Bluetooth o por Wi-Fi:

611. Android proporciona capacidades nativas de *tethering* para Windows Vista/7/8[62] y Linux, pero no así para OS X. Para hacer uso de estas capacidades es necesario conectar el dispositivo móvil al ordenador mediante USB y acceder al menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Anclaje a red y zona Wi-Fi", y en concreto a la opción "Anclaje de USB".

612. A través de la opción "Anclaje de USB" (ver imagen superior) es posible habilitar el servicio de *tethering*, de forma que el ordenador utilice el dispositivo móvil como su conexión de red.

Nota: al habilitar la conexión de red por USB o *tethering*, el modo de depuración, de estar previamente habilitado en Android, será deshabilitado automáticamente.

613. Tras establecerse la conexión de red, y tomando Windows 7 como sistema operativo del ordenador de referencia, se crea automáticamente un interfaz de red de tipo "Remote NDIS based Internet Sharing Service" configurado con una dirección IP dinámica (DHCP) por defecto de clase C (/24), como por ejemplo 192.168.42.17.

[62] Siendo necesaria una configuración adicional en Windows XP (versión ya obsoleta de este sistema operativo).

614. Este interfaz de red NDIS del ordenador tiene asociada una dirección MAC con el OUI "5**6**:1A:D3" (por ejemplo), qué corresponde a una dirección MAC administrada localmente y, por tanto, no asignada a ningún vendedor públicamente.

615. La configuración de este interfaz de red emplea por defecto DHCP (a través del servidor DHCP de Android), y toma todos los valores por defecto existentes en el sistema operativo del ordenador. Así por ejemplo en Windows 7 la pila de comunicaciones de IP versión 6 está activa, al igual que NetBIOS sobre TCP/IP.

616. Se recomienda modificar y restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que se consideren necesarios en el ordenador.

617. El dispositivo móvil, con dirección IP 192.168.42.129, actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

Nota: el direccionamiento IP empleado por Android para la conexión de red compartida a través de USB (192.168.42.x) no puede ser modificado salvo en dispositivos móviles Android *rooted* [Ref.- 96].

618. La dirección MAC asociada al interfaz de red empleado para proporcionar la conexión de red compartida a través de USB por el dispositivo móvil tiene asociado un OUI con valor "c**2**:89:84" (por ejemplo), qué corresponde a una dirección MAC administrada localmente y, por tanto, no asignada a ningún vendedor públicamente.

619. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red del dispositivo móvil empleado para proporcionar la conexión de red compartida a través de USB permite obtener las siguientes conclusiones:

- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por nmap como "dnsmasq 2.51".
- Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).

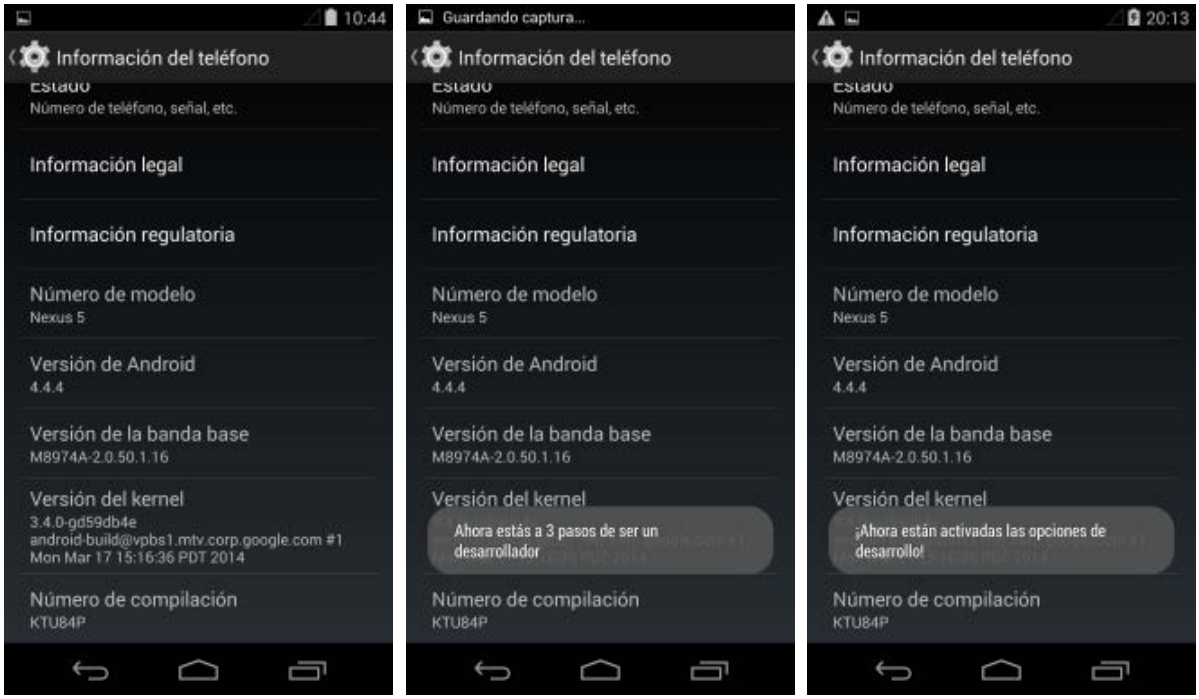
620. Es posible finalizar la compartición de la conexión de datos deshabilitando la opción "Anclaje de USB" habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red compartida.

5.11.3 OPCIONES DE DESARROLLO Y DEPURACIÓN USB

621. Android proporciona acceso a funciones avanzadas y de bajo nivel a través del puerto USB, por ejemplo mediante el Android Debug Bridge (ADB) [Ref.- 107], desde un ordenador. Estas capacidades son normalmente empleadas por los desarrolladores de apps para Android, con el objetivo de llevar a cabo tareas de depuración, mediante el kit de desarrollo de software de Android, SDK (Software Development Kit).

622. Desde la versión 4.2 de Android, el menú que proporciona el acceso para habilitar las opciones de desarrollo está oculto por defecto.

623. Para habilitar dicho menú es necesario acceder al menú "Ajustes [Sistema] - Información del teléfono", y pulsar en siete ocasiones sobre la opción "Número de compilación", disponible en la parte inferior:



624. Al completar las pulsaciones, aparecerá un nuevo menú, "Opciones de desarrollo", en la sección de "Ajustes [Sistema]", antes de la opción "Información del teléfono":

625. A través de este nuevo menú es posible disponer de acceso a múltiples opciones para el desarrollo y depuración de apps en Android, incluyendo la opción "Depuración USB", que permite el acceso a través de USB a las opciones avanzadas de depuración del dispositivo móvil:

626. Desde el punto de vista de seguridad, se recomienda no habilitar las opciones de desarrollo en el dispositivo móvil, y en particular, la opción de depuración a través del puerto USB.

5.11.4 RELACIONES DE CONFIANZA A TRAVÉS DE USB

627. Desde la versión 4.2.2 de Android (Jelly Bean), antes de poder hacer uso de estas capacidades de depuración USB, es necesario establecer una relación de confianza entre el dispositivo móvil y el ordenador conectado a través del puerto USB, permitiendo acceso al terminal a través de una conexión USB de depuración más segura, por ejemplo, mediante ADB [Ref.- 144].

628. El establecimiento de relaciones de confianza a través de USB en Android se ha implementado mediante claves RSA de 2.048 bits. Estas claves son almacenadas en el ordenador bajo "$HOME/.android" en Linux y OS X, o "%USERPROFILE%/.android" en Windows, en los ficheros "adbkey" (clave privada, en formato PEM) y "adbkey.pub" (clave pública, en base64).

629. El dispositivo móvil Android, una vez el usuario acepta una clave de forma permanente, la almacena en el fichero "/data/misc/adb/adb_keys", añadiendo una nueva línea (o entrada) en este fichero correspondiente a la clave contenida en el fichero "adbkey.pub" del ordenador al que se ha conectado por USB:

```
root@hammerhead:/data/misc/adb # ls -l
-rw-r----- system   shell          717 2015-01-19 21:52 adb_keys
root@hammerhead:/data/misc/adb # cat adb_keys
QAAAAHOy...<...>...EAAQA= unknown@unknown
root@hammerhead:/data/misc/adb #
```

630. Este mecanismo de protección no puede ser deshabilitado a través de los ajustes de configuración del dispositivo móvil, opción preferida desde el punto de vista de seguridad.

631. Al habilitar la opción de "Depuración USB", el dispositivo móvil mostrará un mensaje de autorización que deberá ser aprobado por el usuario para poder establecer la conexión a través del puerto USB:

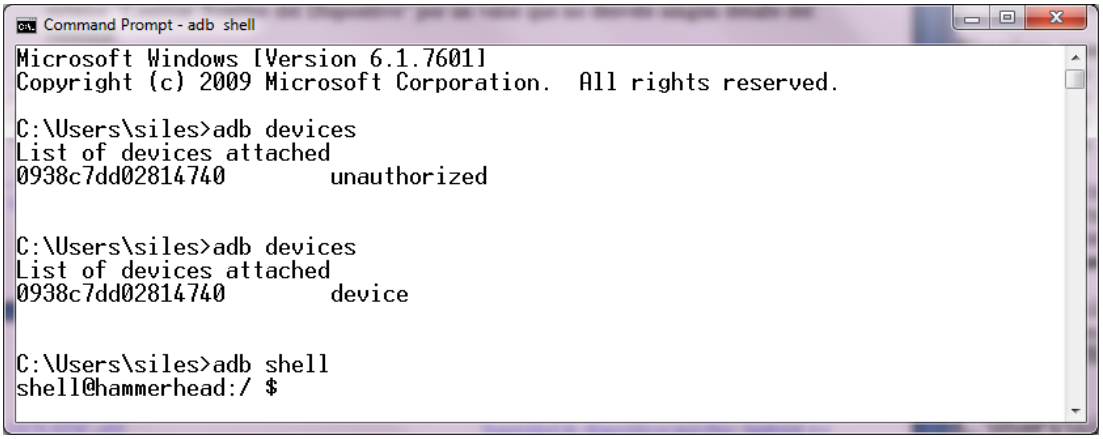
632. El mensaje de autorización muestra el hash MD5 de la clave pública del ordenador con el que se ha establecido la conexión vía USB. Para poder comprobar que el valor mostrado por el dispositivo móvil corresponde con el de la clave pública del ordenador al que está conectado, es necesario obtener el fichero "adbkey.pub" del ordenador y extraer su *hash* MD5. Por ejemplo, en Linux puede emplearse el siguiente comando [Ref.- 144]:

```
$ awk '{print $1}' < adbkey.pub | openssl base64 -A -d -a | openssl md5 -c | \
awk '{print $2}'|tr '[:lower:]' '[:upper:]'
```

633. En el momento de autorizar la relación de confianza, ésta puede permitirse únicamente para la sesión actual (opción por defecto), o de forma permanente, confiando en ese ordenador para futuras conexiones, mediante la opción "Permitir siempre desde este ordenador" (deshabilitada por defecto); ver imagen superior.

634. Este mecanismo de seguridad asegura que sólo ordenadores previamente autorizados por el usuario podrán establecer una conexión mediante el puerto USB cuando el dispositivo móvil está bloqueado y se desconoce el código de acceso.

635. Mientras la relación de confianza no ha sido aprobada, el dispositivo aparece como "unauthorized" en la respuesta del comando "adb devices" (el identificador del dispositivo móvil corresponde a su número de serie):



636. Una vez la relación de confianza ha sido aprobada, el dispositivo aparecerá como disponible, "device", en la respuesta del comando "adb devices" y se podrá acceder a él.

637. En el caso de dispositivos móviles Android multiusuario, únicamente el usuario propietario (o usuario principal) puede autorizar el acceso USB a un ordenador, por lo que para autorizar el mensaje y habilitar la depuración mediante USB es necesario cambiar al usuario principal.

638. Las relaciones de confianza establecidas previamente por USB pueden ser eliminadas en su conjunto, es decir, no selectivamente, mediante el menú "Ajustes [Sistema] - Opciones de desarrollo [Depuración] - Revocar autorizaciones depuración USB":

5.12 COMUNICACIONES NFC

5.12.1 UTILIZACIÓN DE LAS COMUNICACIONES NFC

639. Android dispone de capacidades de comunicación inalámbricas de corto alcance mediante tecnologías NFC (*Near Field Communication*), en concreto en aquellos dispositivos móviles cuyo *hardware* dispone de un interfaz, módulo o controlador NFC.

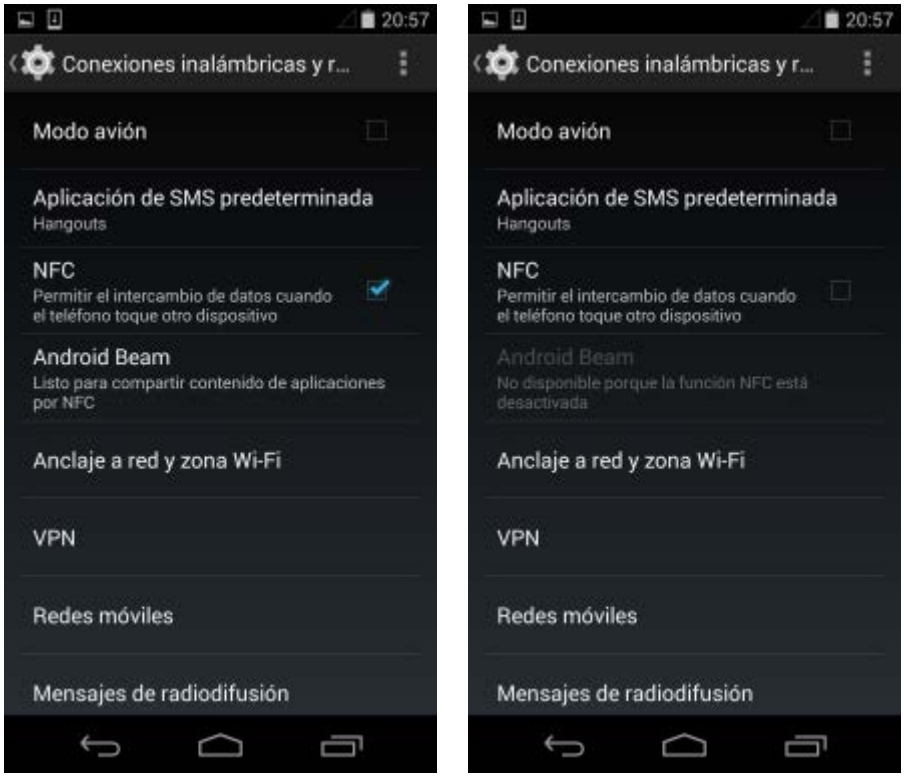
640. El soporte inicial para NFC en Android se introdujo en la versión 2.3, extendiéndose su funcionalidad significativamente en Android 4.4.

641. La principal recomendación de seguridad asociada a las comunicaciones NFC en dispositivos móviles es no activar el interfaz inalámbrico NFC salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el *hardware* del interfaz, el driver o la pila de comunicaciones NFC, incluyendo la funcionalidad adicional implementada sobre NFC, como por ejemplo Android Beam [Ref.- 179].

642. Android no dispone de ninguna indicación en la barra superior de estado, pantalla de inicio o pantalla de bloqueo que indique si el interfaz o controlador NFC está activo, por lo que es necesario acceder a los ajustes de configuración para verificar su estado actual.

5.12.2 CONFIGURACIÓN DE NFC

643. El interfaz inalámbrico NFC puede ser desactivado en Android, ya que está habilitado por defecto, a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más", y en concreto a través de la opción "NFC":

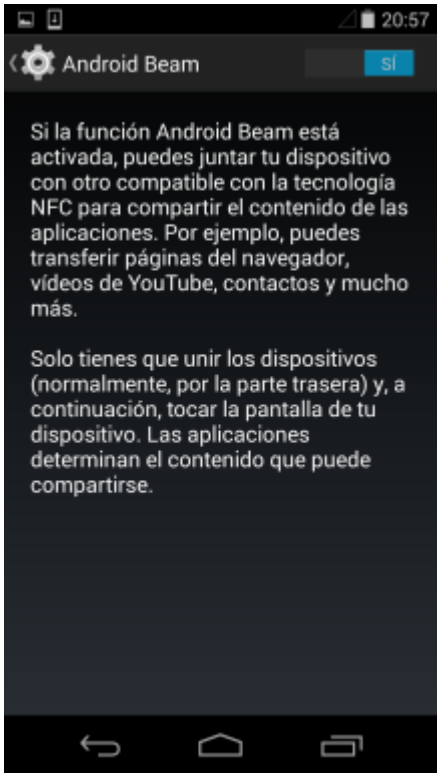


644. Desafortunadamente, Android no proporciona a través del interfaz de usuario acceso a otros ajustes de configuración más avanzados relacionados con NFC.

645. Por otro lado, Android permite compartir contenidos mediante NFC entre dos dispositivos móviles, tales como páginas web, fotografías, vídeos, contactos, enlaces a apps en Google

Play, ubicaciones en "Maps" y otros datos, a través de Android Beam (habilitado por defecto y disponible desde la versión 4.0 de Android). El proceso de transmisión se lleva a cabo al aproximar el interfaz NFC de ambos dispositivos móviles, normalmente situado en la parte trasera de los mismos.

646. Para ello es necesario que los dos dispositivos móviles dispongan del interfaz NFC activo, así como de la funcionalidad Android Beam habilitada [Ref.- 179]. Android Beam puede ser habilitado a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más" y la opción "Android Beam" (junto al botón "[SI | NO]" asociado), debiendo estar la opción "NFC" activa previamente:



647. Para compartir el contenido sólo es necesario disponer de la app con el contenido a intercambiar abierta, aproximar los dos dispositivos móviles, y autorizar la transmisión de datos mediante la opción "Toca para compartir", seleccionada desde el dispositivo emisor.

648. En el ejemplo inferior, el dispositivo móvil emisor tiene el navegador web abierto en una página web concreta, se aproxima al dispositivo móvil receptor, mediante una señal acústica se confirma a los usuarios que se ha establecido la conexión NFC, y tras ser autorizada la transacción por el usuario del dispositivo móvil emisor (mediante el botón "Toca para compartir"), el receptor recibe la URL asociada a dicha página web y ésta es automáticamente es abierta en su navegador web:

5.12.3 PAGOS (Y OTROS SERVICIOS) MEDIANTE NFC

649. En versiones previas de Android, la utilización del dispositivo móvil para la realización de pagos, por ejemplo mediante Google Wallet[63] (disponible desde septiembre de 2011 en USA), no tuvo una aceptación muy extendida, principalmente porque era necesario disponer de una adecuada integración entre Android (software) y el controlador NFC del dispositivo móvil (hardware), y de acceso al *Secure Element* (SE) existente en el dispositivo móvil. En muchos modelos de terminal este acceso estaba limitado o restringido, especialmente la instalación de nuevas *applets* en el SE.

650. El *Secure Element* (SE) es un componente *hardware* (implementado como el chip de las tarjetas inteligentes, o *smartcards*) que proporciona tanto capacidades de almacenamiento seguro, para por ejemplo guardar claves de autentificación u otro material sensible, como un entorno de ejecución seguro, para la ejecución de código y tareas críticas.

651. El SE suele estar integrado en los dispositivos móviles actuales como una *Universal Integrated Circuit Card* (UUIC, es decir, una tarjeta SIM), embebido en el propio hardware del terminal, o a través de una tarjeta SD especial. Si el dispositivo móvil dispone de soporte para NFC, el SE normalmente está embebido en el terminal y conectado al controlador NFC.

652. Dentro de la gama de dispositivos móviles Nexus de Google, el primer modelo con capacidades NFC fue el Nexus S, seguido de sus sucesores el Galaxy Nexus y el Nexus 4. Todos estos modelos, además de disponer de un interfaz o controlador NFC, disponían de un SE embebido (denominado eSE, *embedded SE*).

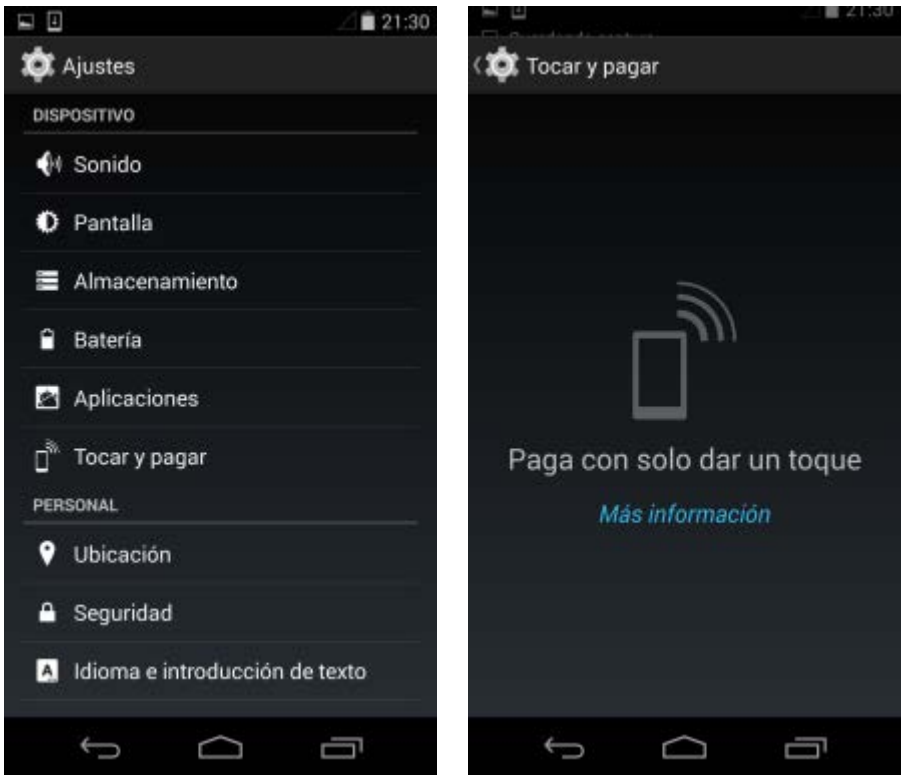
[63] https://wallet.google.com

653. Android, desde la versión 4.4 (KitKat), implementa una nueva arquitectura más abierta para realizar pagos NFC, que funciona con cualquier operador móvil y que permite a las apps gestionar la información sobre pagos en "la nube" o en cualquier dispositivo móvil.

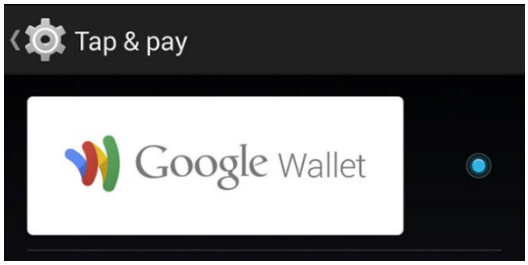
654. Estas capacidades permiten (por ejemplo a los dispositivos móviles Nexus de Google) "Tocar y pagar" (Tap & Pay), por ejemplo con Google Wallet (únicamente disponible en USA actualmente), o mediante otras apps, en tiendas que admiten pagos sin contacto (*contactless*):

655. Adicionalmente, NFC puede ser empleado para gestionar las tarjetas de fidelización, tarjetas de transporte, tarjetas de identificación y otros servicios similares.

656. La funcionalidad de "Tocar y pagar" (Tap & Pay) [Ref.- 180] está disponible a través del menú de "Ajustes [Dispositivo] - Tocar y pagar":



657. Para poder hacer uso de esta funcionalidad es necesario disponer de al menos una app compatible con "Tocar y pagar", qué aparecerá en esta pantalla de configuración, habiendo seleccionado previamente una de las apps compatibles como app predeterminada para "Tocar y pagar" (ejemplo en inglés):



658. "Tocar y pagar" puede ser deshabilitado desde la app de pago asociada (si dispone de esta posibilidad), o en su defecto, deshabilitando el interfaz NFC en Android.

659. Desde abril de 2014, Google Wallet sólo está disponible en Android 4.4 o superior, y hace uso de HCE (descrito posteriormente) en lugar de SE. Adicionalmente a Google Wallet (USA), otras apps que se integran con esta funcionalidad son las asociadas a entidades financieras que hacen uso de los servicios Visa payWave y Mastercard paypass[64].

660. El acceso al interfaz NFC desde el punto de vista de los permisos de Android durante el proceso de instalación de las apps con estas capacidades, se verá reflejado (potencialmente) en el grupo "Otros" como "controlador Comunicación de campo cercano (NFC)"[65]:

661. Desde Android 4.4 (KitKat), Android dispone de soporte para *Host Card Emulation* (HCE) [Ref.- 178]. Mediante HCE cualquier app en Android puede emular una tarjeta NFC

[64] http://www.xatakandroid.com/mercado/visa-y-mastercard-usaran-host-card-emulation-para-pagos-moviles-nfc-con-android-4-4-kitkat
[65] http://www.blogbbva.es/bbva-wallet-nfc-2/

(*smartcard*)[66], y por tanto iniciar transacciones NFC, no siendo necesario obligatoriamente hacer uso del *Secure Element* (SE) y de las *applets* instaladas en el propio SE.

662. Anteriormente sólo era posible hacer uso del modo de emulación de tarjeta si se hacía uso del SE conectado al controlador NFC. Con HCE, las apps actúan como tarjetas sin contacto virtuales (*virtual contactless smartcards*).

663. Adicionalmente a HCE, las apps puede funcionar en modo lectura (*Reader Mode*) con capacidades directas de lectura de tarjetas NFC cuando las apps ejecutan en primer plano, o en modo P2P (*Point-to-Point*) con funcionalidad básica de intercambio de datos.

664. Por otro lado, las apps pueden declarar el tipo de etiquetas NFC (*tags*) en las que están interesadas, en función de la tecnología de las etiquetas, y cuando el servicio de NFC de Android descubre una nueva etiqueta NFC, enruta la petición para su procesamiento a la app (o apps) correspondientes previamente registradas [Ref.- 157].

665. Debido al soporte para HCE introducido por Android desde la versión 4.4, los nuevos modelos de dispositivos móviles Nexus de Google, como el Nexus 5 o el Nexus 7 (2013), no disponen de un SE embebido (en favor de HCE).

666. Desde el punto de vista de seguridad, y debido al tipo de información sensible y de transacciones y pagos asociada a esta funcionalidad, se recomienda deshabilitar el interfaz NFC y las opciones o servicios adicionales (Android Beam, "Tocar y pagar", etc), salvo que se quiera hacer un eso explícito y controlado de los mismos.

667. Aunque más incomodo para el usuario, se recomienda habilitar temporalmente estas capacidades únicamente en el momento de ir a hacer uso de las mismas, volviendo a deshabilitar el interfaz NFC tan pronto se haya completado la transacción o el intercambio de datos mediante esta tecnología inalámbrica.

5.13 COMUNICACIONES BLUETOOTH

5.13.1 UTILIZACIÓN DE LAS COMUNICACIONES BLUETOOTH

668. La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (802.15) en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles [Ref.- 51].

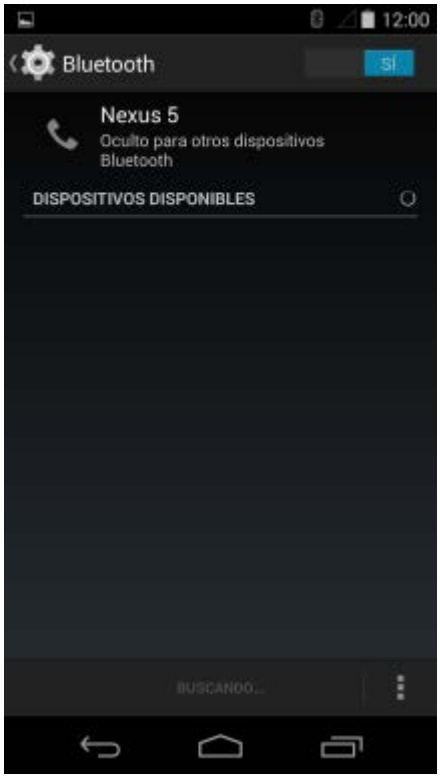
[66] Android HCE emula tarjetas ISO/IEC 7816 que hacen uso del protocolo ISO/IEC 14443-4 (ISO-DEP) para las trasmisiones sin contacto (*contactless*).

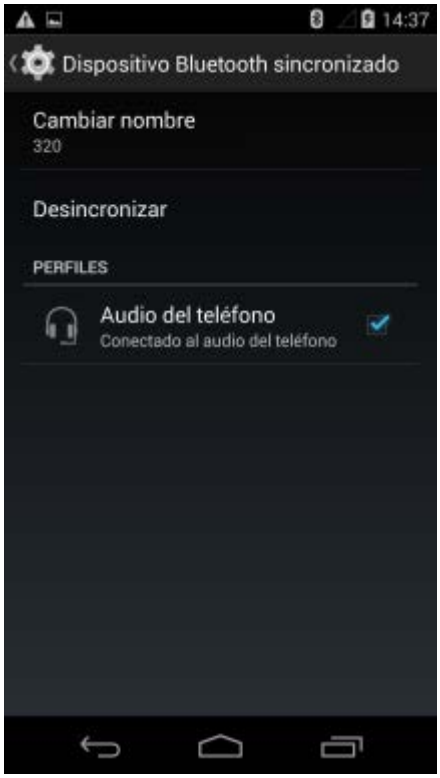
669. El interfaz inalámbrico Bluetooth puede ser desactivado en Android, situación por defecto, a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth"[67], mediante el botón "SÍ|NO" de la opción "Bluetooth".

670. El estado del interfaz Bluetooth puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado, ya que tan pronto el interfaz está activo, se mostrará el icono de Bluetooth (de color gris); ver imagen inferior izquierda.

671. Android proporciona información en la barra superior de estado sobre el estado del interfaz Bluetooth, y si existe una conexión establecida actualmente (el icono de Bluetooth estará iluminado de color blanco), a través de un conjunto específico de iconos que muestran el logotipo de Bluetooth. Por ejemplo:

[67] A partir de este momento, por simplificar, el menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth" se abreviará como "Ajustes - Bluetooth".





672. Adicionalmente desde los ajustes rápidos, o desde el menú de "Ajustes" (pero éste no permite un acceso sencillo, ágil y rápido), es posible ver el estado actual del interfaz Bluetooth: "Bluetooth" (indica que el interfaz está activado) o "Bluetooth Desactivado".

673. Android mantiene el estado del interfaz Bluetooth tras reiniciar el dispositivo móvil, es decir, si el interfaz Bluetooth estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo.

674. La activación inicial del interfaz Bluetooth se llevará a cabo tan pronto el dispositivo móvil se haya reiniciado, incluso aunque aún no haya sido desbloqueado por primera vez tras encenderlo (igual que el interfaz Wi-Fi; ver apartado "5.14. Comunicaciones Wi-Fi").

675. Igualmente, al salir del modo avión el estado del interfaz Bluetooth será restaurado, activándose de nuevo en el caso de haber estado activo previamente (antes de activar el modo avión).

676. El interfaz Bluetooth también permanece activo cuando el dispositivo móvil está en espera o *stand-by*, es decir, encendido pero con la pantalla apagada y bloqueado.

Nota: tras un restablecimiento de fábrica, o *hard-reset*, el interfaz Bluetooth del dispositivo móvil empleado para la elaboración de la presente guía está deshabilitado por defecto. Una vez el interfaz es habilitado por el usuario, éste responde a peticiones Bluetooth (en modo oculto o no visible por defecto).

677. La dirección del interfaz Bluetooth, BD_ADDR (Bluetooth Device Address) está disponible a través del menú "Ajustes - Información del teléfono - Estado", y en concreto, en el campo "Dirección de Bluetooth". La dirección no es visible, se muestra el mensaje "No disponible" en su lugar, si el interfaz Bluetooth no se encuentra activo:

Nota: la parte de la dirección Bluetooth (BD_ADDR) asociada al fabricante, NAP+UAP (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor "64:89:9A" está asignado por el IEEE (http://standards.ieee.org/regauth/oui/index.shtml) a "LG":

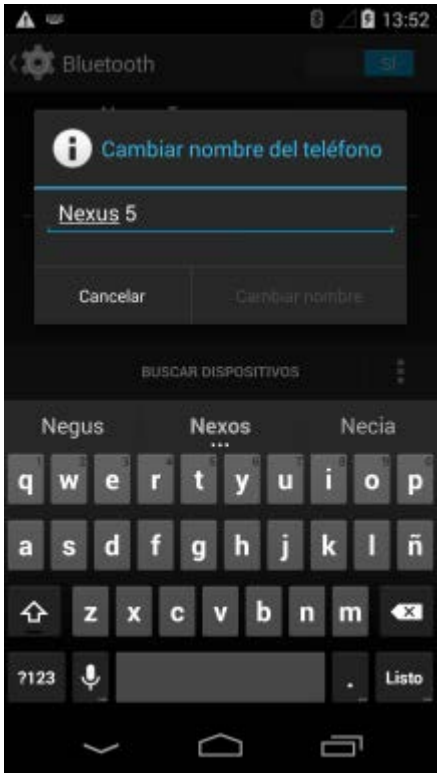
```
64-89-9A   (hex)            LG Electronics
64899A     (base 16)        LG Electronics
                            60-39, Gasan-dong, Geumcheon-gu
                            Seoul Seoul 153-801
                            KOREA, REPUBLIC OF
```

5.13.2 CONFIGURACIÓN GENERAL DE BLUETOOTH

678. Debe tenerse en cuenta que, al igual que para el interfaz Wi-Fi, para poder llevar a cabo la configuración de la pila de comunicaciones Bluetooth a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz (como se muestra en las dos siguientes imágenes, salvo para ver los archivos recibidos) por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:

679. La pantalla de configuración (junto a las opciones avanzadas disponibles desde el botón "...") permite llevar a cabo múltiples acciones, como habilitar y deshabilitar el interfaz Bluetooth, configurar el nombre del dispositivo móvil empleado para las conexiones Bluetooth, configurar el estado del interfaz Bluetooth (oculto o visible) y el tiempo de visibilidad, mostrar los archivos recibidos por Bluetooth o buscar otros dispositivos Bluetooth con los que conectarse:

680. En caso de no especificar ningún nombre para Bluetooth, el valor por defecto empleado como nombre de dispositivo móvil para las conexiones Bluetooth por Android es "Nexus 5" (correspondiente al tipo y modelo exacto de dispositivo móvil empleado para la elaboración de la presente guía), tal como se indica en el menú correspondiente a "Cambiar nombre del teléfono" en los ajustes de Bluetooth:

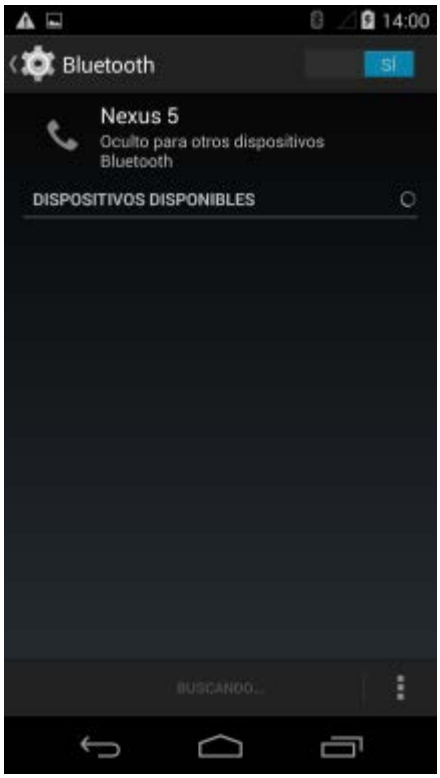


681. Debido a que el nombre por defecto desvela el tipo de dispositivo móvil empleado, se recomienda modificarlo por un valor que no revele detalles ni del dispositivo móvil

(fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociadas al mismo), como por ejemplo "bt0001" ("Bluetooth device 0001").

682. En el caso de activar el interfaz Bluetooth para hacer uso de esta tecnología, se recomienda configurar el mismo en modo oculto o no visible, con el objetivo de no desvelar su presencia frente a las operaciones de búsqueda de otros dispositivos Bluetooth.

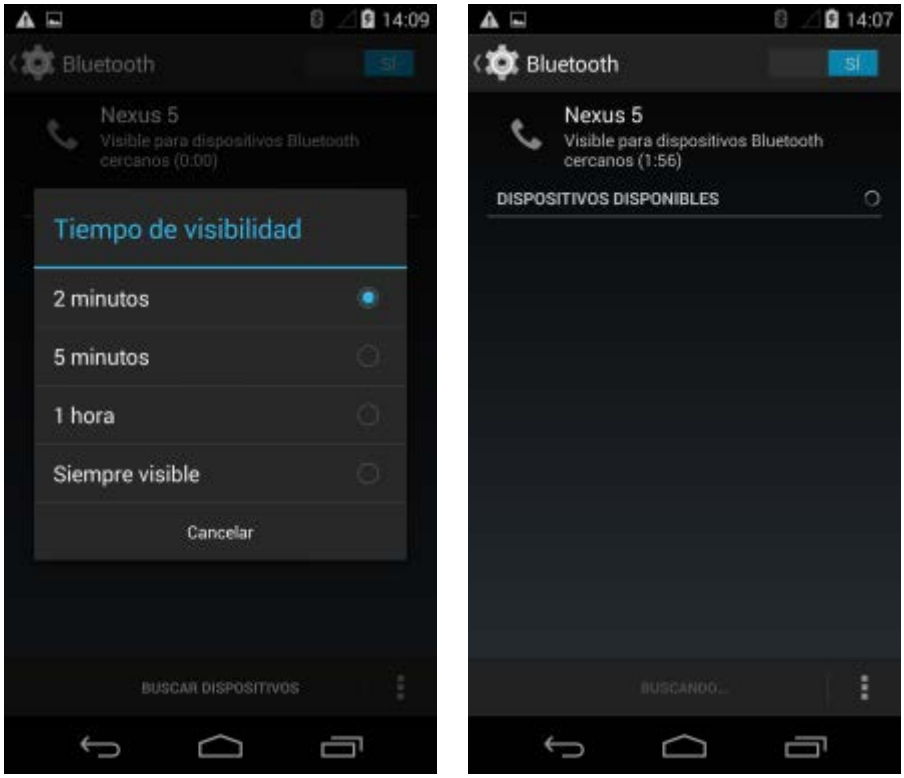
683. Por defecto, al activar el interfaz Bluetooth, éste se encuentra en modo oculto o no visible, opción recomendada desde el punto de vista de seguridad, tal como se detalla en el texto bajo el nombre del dispositivo:



684. Desde la ventana de configuración de Bluetooth, accesible a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth"[68], no debe seleccionarse el nombre del dispositivo, ya que cambiará su estado a visible durante el tiempo configurado actualmente.

685. La cantidad de tiempo que el dispositivo permanecerá en estado visible se puede configurar desde el menú "Ajustes - Bluetooth - [...] - Tiempo de visibilidad". Al configurar el interfaz Bluetooth en el estado visible, el dispositivo permanecerá en dicho estado por defecto únicamente durante los próximos 120 segundos (2 minutos) tras seleccionar su nombre, volviendo al modo oculto automáticamente tras ese periodo de tiempo. Sin embargo, es posible extender ese tiempo a 5 minutos, 1 hora o que siempre esté en estado visible (opciones desaconsejadas desde el punto de vista de seguridad):

[68] A partir de este momento, por simplificar, el menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth" se abreviará como "Ajustes - Bluetooth".



686. Se recomienda configurar la visibilidad del dispositivo al mínimo tiempo necesario para realizar el emparejamiento, en caso de configurar como visible el dispositivo móvil (y no el otro dispositivo Bluetooth, ya que sólo es necesario que uno de los dos dispositivos se encuentre en estado visible para establecer el emparejamiento inicial).

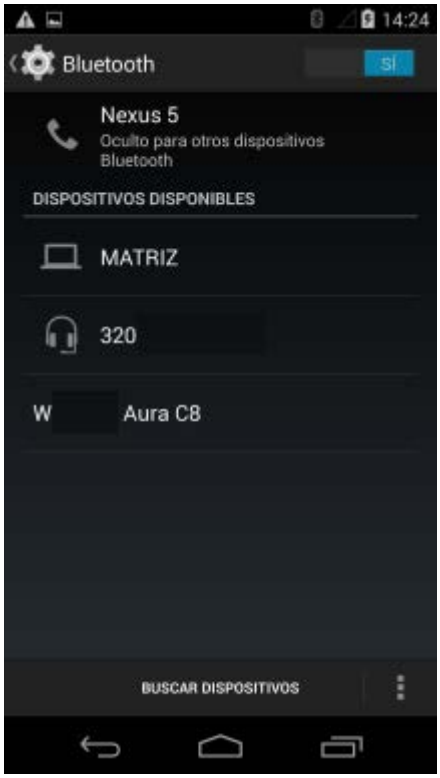
687. Al encontrarse el interfaz Bluetooth del dispositivo móvil en modo oculto, todas las conexiones Bluetooth y operaciones de emparejamiento con otros dispositivos deberán iniciarse desde el dispositivo móvil, siendo necesario que el otro dispositivo Bluetooth se encuentre en modo visible.

Nota: en el caso de requerir, de forma excepcional, disponer del interfaz Bluetooth en modo visible para realizar el emparejamiento con otro dispositivo, la opción de estar visible sólo temporalmente durante 120 segundos es la opción recomendada desde el punto de vista de seguridad, con el objetivo de volver al estado oculto tras la operación de emparejamiento.

Actualmente, pero no disponible en versiones previas de Android, se dispone de la opción para que el dispositivo móvil se encuentre visible de forma permanente [Ref.- 123].

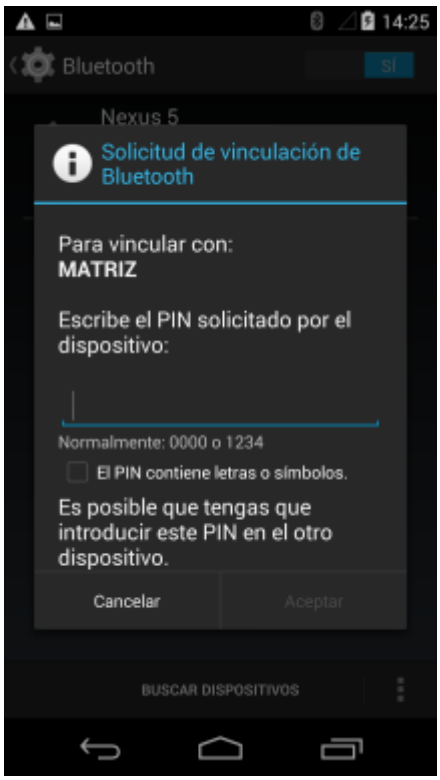
5.13.3 DISPOSITIVOS BLUETOOTH EMPAREJADOS

688. Android lleva a cabo de forma automática búsquedas de dispositivos Bluetooth visibles (por ejemplo al habilitar el interfaz Bluetooth), proceso indicado por el texto "Buscando…" y una rueda giratoria en la parte derecha, mostrando los mismos bajo la sección "Dispositivos Disponibles" de la pantalla de configuración de Bluetooth:

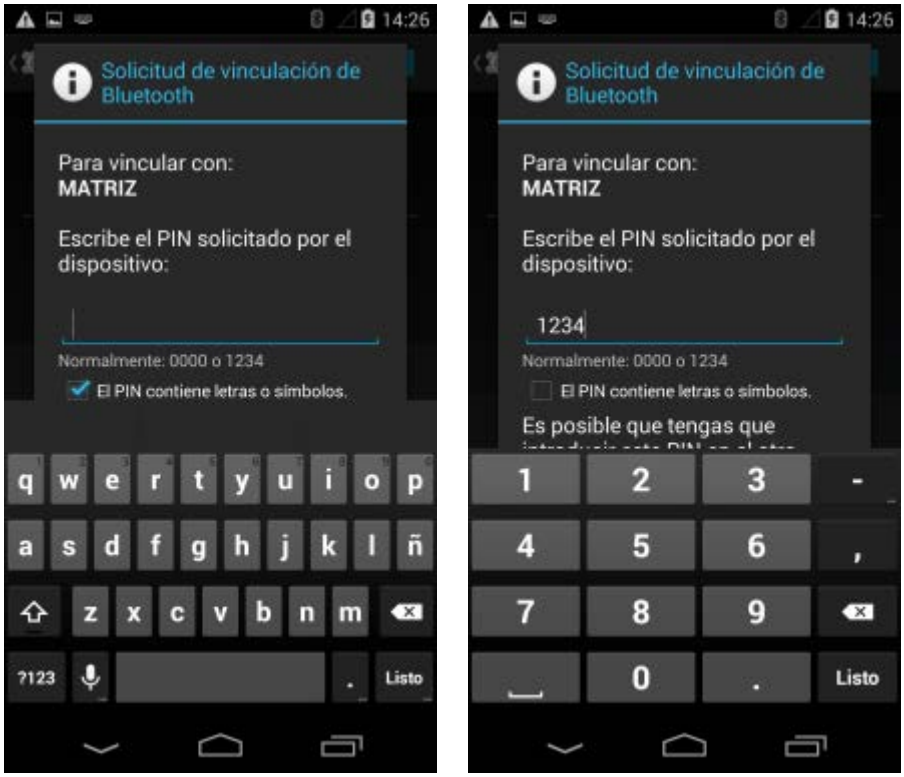


689. La operación de búsqueda puede realizarse también de forma manual mediante la opción "Buscar dispositivos" disponible en la zona inferior.

690. Mediante la selección de un dispositivo visible de la lista es posible realizar el emparejamiento con el mismo. Android establecerá la comunicación Bluetooth con el otro dispositivo y llevará a cabo el proceso de emparejamiento, solicitando al usuario el PIN o contraseña Bluetooth:



691. Android permite la utilización de PINs o contraseñas Bluetooth formados por caracteres alfanuméricos y símbolos (mediante la opción "El PIN contiene letras o símbolos"), de hasta 16 caracteres de longitud, durante el emparejamiento con otros dispositivos (tal como define la especificación Bluetooth):

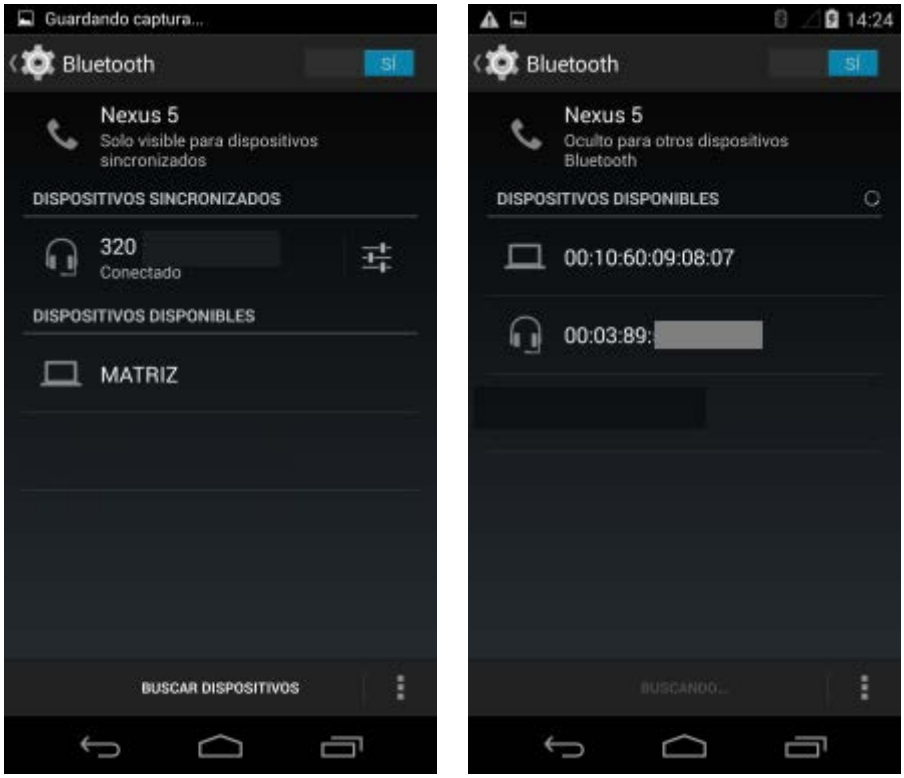


692. El uso de contraseñas alfanuméricas constituye la opción recomendada desde el punto de vista de seguridad, frente a PINs sólo basados en dígitos.

693. La contraseña o PIN Bluetooth se mostrará en la pantalla al ser introducida por el usuario (ver imagen superior derecha), sin disponer Android de ninguna opción para ocultar su valor, por ejemplo mediante el carácter asterisco ("*"), por lo que debe prestarse especial atención a que nadie, aparte del usuario, disponga de acceso visual a la pantalla durante el proceso de emparejamiento.

694. Se recomienda hacer uso de contraseñas alfanuméricas robustas para el emparejamiento con otros dispositivos Bluetooth (compuestas por números, letras y símbolos, y de al menos 8 caracteres), en lugar de emplear un PIN de cuatro dígitos (valor común por defecto y empleado de forma estándar en el emparejamiento de dispositivos Bluetooth; y en ningún caso utilizar los valores 0000 o 1234 sugeridos por Android).

695. Una vez se ha realizado la vinculación o emparejamiento con otro dispositivo, éste será mostrado bajo la sección "Dispositivos Sincronizados" de la pantalla de configuración de Bluetooth:



696. No se han identificado opciones en Android para poder consultar y obtener la dirección Bluetooth (BD_ADDR) de cada dispositivo con el que se ha realizado el emparejamiento, muy útil a la hora de reconocer otros dispositivos asociados al terminal, así como modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones con el dispositivo móvil deben ser autorizadas.

697. La dirección Bluetooth está sólo disponible momentáneamente durante el proceso inicial de descubrimiento, y antes de que se obtenga el nombre de los otros dispositivos Bluetooth (ver imagen superior derecha).

5.13.4 CONFIGURACIÓN AVANZADA DE BLUETOOTH

698. La implementación de Bluetooth de Android, por defecto incluye diferentes perfiles en el caso de la versión y dispositivo móvil empleados para la elaboración de la presente guía: "Headset Gateway", "Handsfree Gateway", "AV Remote Control Target", "Advanced Audio", "Android Network Access Point", "Android Network User", "MAP SMS" (Message Access Profile)[69], "OBEX Phonebook Access Server" y "OBEX Push".

699. No se han identificado en Android opciones de configuración avanzadas que permitan establecer restricciones de conectividad (autentificación, autorización y/o cifrado), obtener información, o configurar opciones específicas, para los diferentes perfiles Bluetooth disponibles (como por ejemplo para la configuración de red, de audio, de transferencia de archivos, etc).

[69] El perfil de Bluetooth MAP permite al dispositivo móvil intercambiar mensajes con vehículos equipados con tecnología Bluetooth.

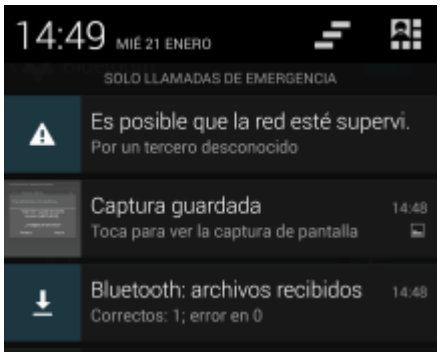
5.13.5 OBEX PUSH

700. Android dispone por defecto de capacidades para el intercambio de objetos, asociadas al perfil Bluetooth estándar OBEX Push (en ocasiones referenciado como OBEX Object Push).

701. El perfil de recepción de objetos (OBEX - *Object Exchange*- Push) a través de Bluetooth está habilitado por defecto y no se ha identificado ninguna opción de configuración para deshabilitarlo.

702. Cuando otro dispositivo Bluetooth se comunica con este perfil e intenta enviar un objeto (por ejemplo, un archivo), Android solicita autorización por parte del usuario a través de una notificación vía la barra superior de estado antes de permitir la operación de intercambio:

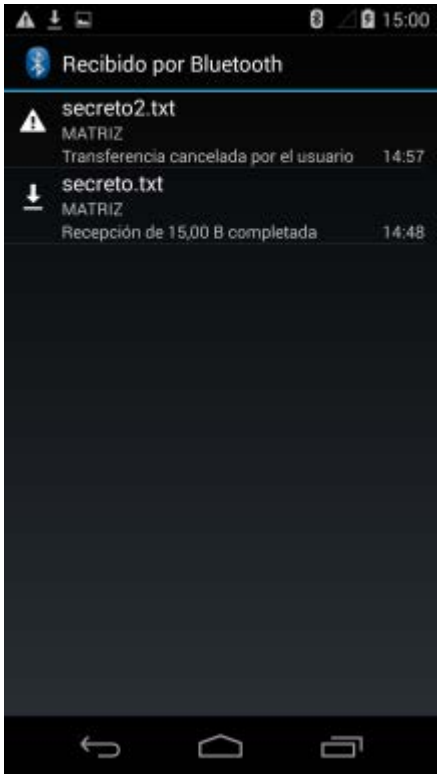
703. Mediante la selección de dicha notificación, el usuario es informado sobre los detalles de la transferencia, que incluyen el nombre del dispositivo Bluetooth remitente, el nombre los datos transferidos (nombre del archivo), y el tamaño:



704. Si la transferencia de datos a través del perfil OBEX Push tiene éxito, tras emplearse los mecanismos de autorización por parte del usuario descritos, se indica el resultado al usuario mediante otra notificación de confirmación (desde la que es también posible acceder directamente al archivo).

705. El objeto (o fichero) recibido se almacena por defecto en el directorio "bluetooth" del área de almacenamiento interno del dispositivo móvil.

706. El acceso a los archivos recibidos mediante Bluetooth está disponible desde "Ajustes - Bluetooth - [...] - Mostrar archivos recibidos", incluyendo tanto los que han tenido éxito como los intentos cancelados o rechazados por el usuario:

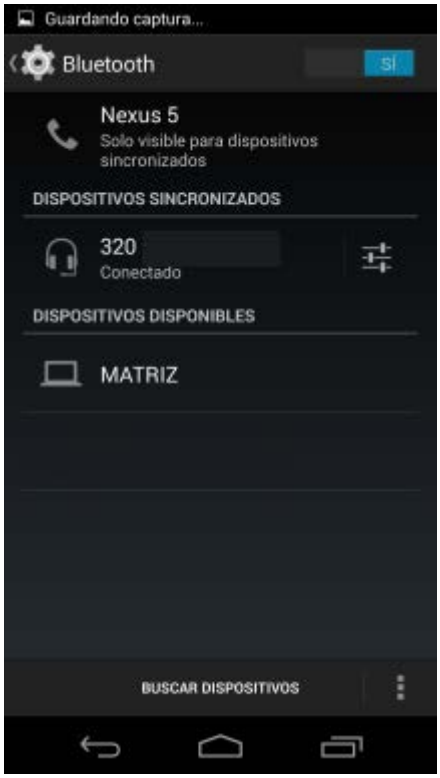


707. El perfil OBEX Push no dispone del mecanismo de autentificación habilitado por defecto, debido a su modelo de uso, en el que no es necesario emparejarse previamente con el otro dispositivo para transferir datos (u objetos, OBEX).

708. El comportamiento de solicitud de autorización al usuario descrito previamente se presenta tanto con dispositivos Bluetooth con los que previamente se ha emparejado Android (es decir, autentificados), como con dispositivos nuevos.

5.13.6 MANOS LIBRES BLUETOOTH

709. El emparejamiento con dispositivos Bluetooth manos libres puede no requerir el introducir ningún PIN o contraseña, proceso conocido como emparejamiento automático o *auto pairing*, debido a que Android dispone de conocimiento de los PINs empleados por defecto (no modificables) por los fabricantes de manos libres Bluetooth:



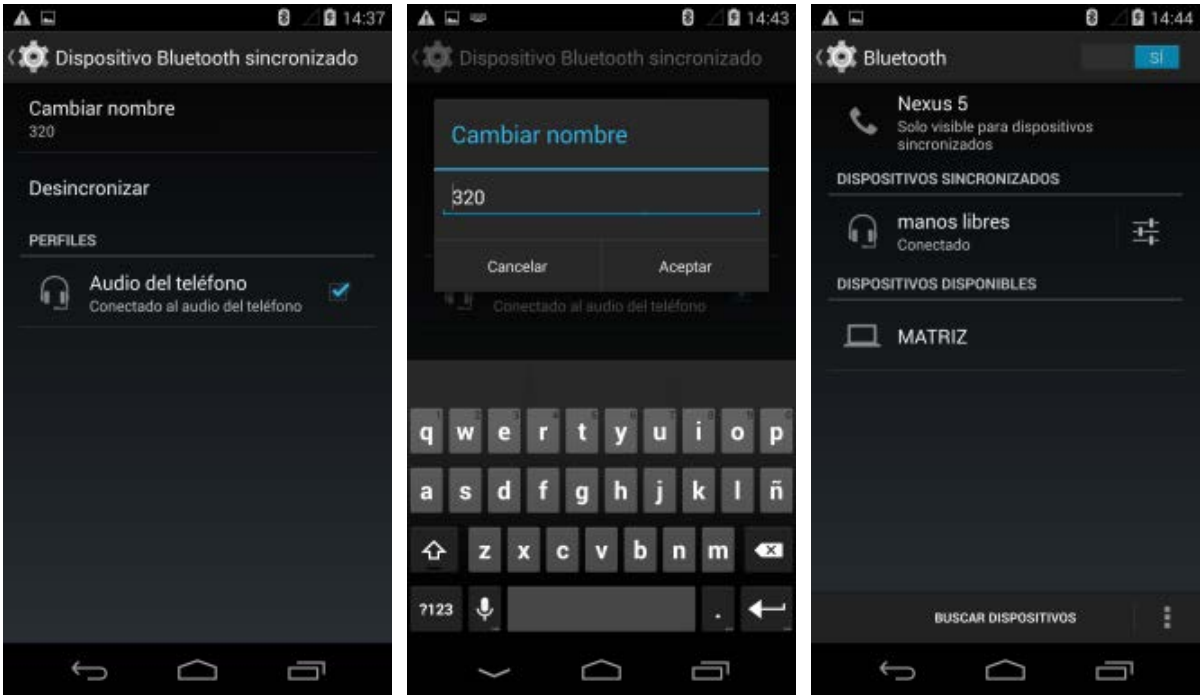
710. El emparejamiento automático se lleva a cabo por ejemplo con dispositivos que emplean valores de PIN por defecto, como por ejemplo "0000".

711. Una vez vinculado el dispositivo móvil con un dispositivo manos libres, el interfaz Bluetooth del dispositivo móvil, cada vez que es habilitado, intenta establecer automáticamente una conexión con los dispositivos manos libres disponibles en la lista de dispositivos emparejados, proceso conocido como conexión automática o *auto connect*. Si el dispositivo Bluetooth se encuentra en el rango de alcance del dispositivo móvil, y fueron emparejados previamente, se establecerá la conexión, estado identificado en Android por el icono de estado de Bluetooth en la barra superior de estado.

712. El proceso de conexión automática no tiene asociada ninguna solicitud de confirmación por parte del usuario ni puede ser deshabilitado mediante opciones de configuración.

713. Una vez se ha establecido la conexión Bluetooth con otro dispositivo, al seleccionarlo es posible desconectarse del mismo, mediante el botón "Aceptar":

714. Una vez se ha establecido la conexión Bluetooth con otro dispositivo (independientemente de su tipo o del perfil empleado), al seleccionar su botón de configuración asociado (disponible en la parte derecha, junto a su nombre), se dispone de un menú de opciones. A través del mismo es posible modificar el nombre empleado localmente para identificar al otro dispositivo, eliminar la vinculación o emparejamiento previos mediante el botón "Desincronizar", o seleccionar los perfiles ofrecidos por el otro dispositivo que se desean utilizar:



715. No se han identificado en Android opciones de configuración avanzadas que permitan configurar los perfiles de Bluetooth asociados a la conexión con dispositivos manos libres.

5.13.7 CONEXIÓN DE RED COMPARTIDA POR BLUETOOTH

Android proporciona capacidades nativas de *tethering* a través de USB (ver apartado "5.11.2. Conexión de de red compartida por USB (*Tethering*)"), Bluetooth y Wi-Fi (ver apartado "5.14. Comunicaciones Wi-Fi").

716. Para hacer uso de estas capacidades mediante Bluetooth (Personal Area Network, PAN) es necesario acceder al menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Anclaje a red y zona Wi-Fi", y en concreto a la opción "Anclaje de Bluetooth":

717. A través de la opción "Anclaje de Bluetooth" es posible habilitar el servicio de *tethering*, de forma que el ordenador utilice el dispositivo móvil como su conexión de red a través de una conexión Bluetooth. Para ello es necesario que previamente el ordenador y el dispositivo móvil se hayan emparejado.

718. La configuración empleada para Bluetooth es similar a la utilizada para compartir la conexión mediante USB (ver apartado "5.11.2. Conexión de de red compartida por USB (*Tethering*)") o Wi-Fi (ver apartado "5.14.6. Punto de acceso o zona Wi-Fi").

719. Tras establecerse la conexión de red, y tomando Windows 7 como sistema operativo del ordenador de referencia, se crea automáticamente un interfaz de red de tipo "Bluetooth Device (Personal Area Network)" (PAN) configurado con una dirección IP dinámica (DHCP) por defecto de clase C (/24), como por ejemplo 192.168.44.17.

720. Este interfaz de red Bluetooth del ordenador tiene asociada la dirección MAC del adaptador Bluetooth empleado en el ordenador.

721. La configuración de este interfaz de red emplea por defecto DHCP (a través del servidor DHCP de Android), y toma todos los valores por defecto existentes en el sistema operativo del ordenador. Así por ejemplo en Windows 7 la pila de comunicaciones de IP versión 6 está activa, al igual que NetBIOS sobre TCP/IP.

722. Se recomienda modificar y restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que se consideren necesarios en el ordenador.

723. El dispositivo móvil, con dirección IP 192.168.44.1, actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

Nota: el direccionamiento IP empleado por Android para la conexión de red compartida a través de Bluetooth (192.168.44.x) no puede ser modificado salvo en dispositivos móviles *rooted* [Ref.- 96].

724. La dirección MAC asociada al interfaz de red empleado para proporcionar la conexión de red compartida a través de USB por el dispositivo móvil tiene asociada la dirección MAC del interfaz Bluetooth del dispositivo móvil.

725. Es posible finalizar la compartición de la conexión de datos deshabilitando la opción "Anclaje de USB" habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red compartida.

5.14 COMUNICACIONES WI-FI

5.14.1 UTILIZACIÓN Y CONFIGURACIÓN DE LAS COMUNICACIONES WI-FI

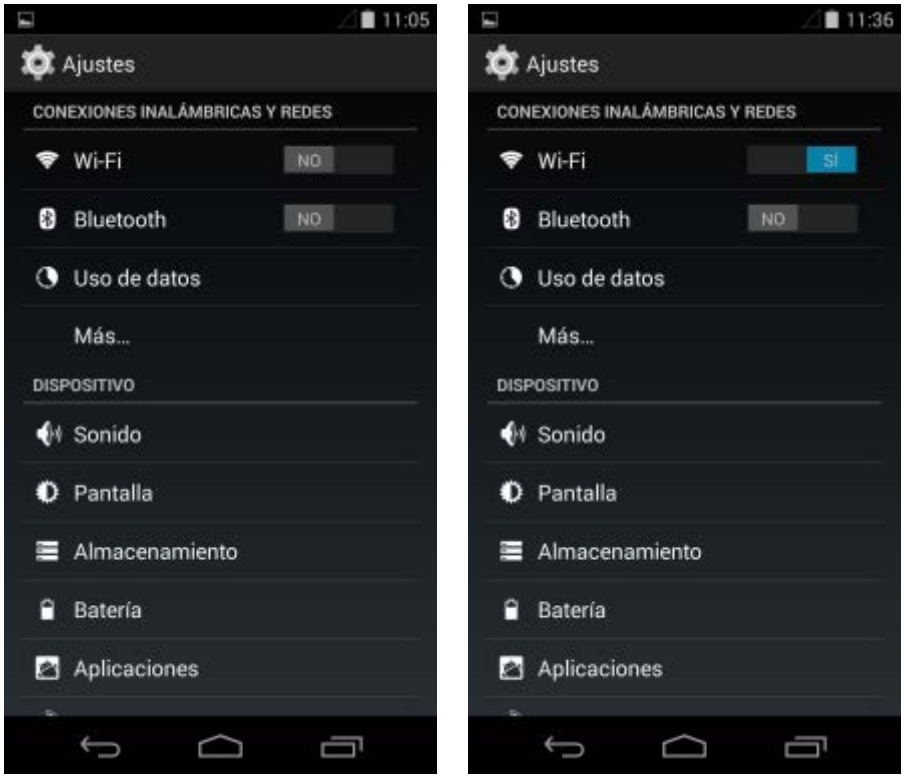
726. La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (802.11) en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi [Ref.- 49].

Nota: durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal; ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial"), tanto si se omite el establecimiento de una conexión a una red Wi-Fi, como si no, el interfaz Wi-Fi estará habilitado por defecto.

Desde el punto de vista de seguridad se recomienda deshabilitar el interfaz Wi-Fi y habilitarlo posteriormente, una vez el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión a una red Wi-Fi.

727. El interfaz inalámbrico Wi-Fi puede ser desactivado en Android a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi"[70], mediante el botón "SÍ|NO" de la opción "Wi-Fi":

[70] A partir de este momento, por simplificar, el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi" se abreviará como "Ajustes - Wi-Fi".



728. Android proporciona información en la barra superior de estado sobre la disponibilidad de redes Wi-Fi abiertas y si se está o no conectado a una red Wi-Fi actualmente, a través de un conjunto específico de iconos que muestran las ondas de las señales Wi-Fi:

729. La disponibilidad de redes Wi-Fi abiertas se muestra con un símbolo de interrogación en las ondas de las señales Wi-Fi, en la zona izquierda de la barra superior de estado (correspondiente a las notificaciones), acompañado de un nuevo mensaje de notificación:

730. La notificación respecto a la disponibilidad de redes Wi-Fi abiertas puede ser configurada a través del menú "Ajustes - Wi-Fi - [...] - Ajustes avanzados", y en concreto mediante la opción "Notificación de red disponible" (habilitada por defecto). Esta opción puede ser modificada únicamente una vez el interfaz Wi-Fi ha sido habilitado:

731. Dado que desde el punto de vista de seguridad se desaconseja el establecer conexiones con redes Wi-Fi abiertas, se recomienda desactivar esta opción de notificación.

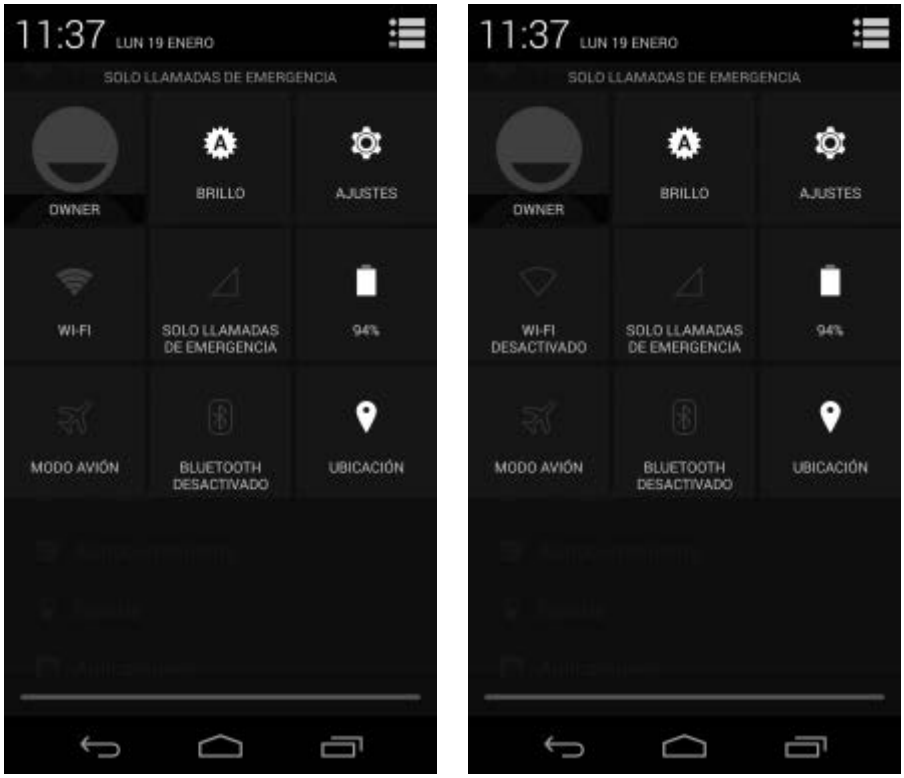
732. Los ajustes rápidos, disponibles al desplazar hacia abajo con dos dedos la barra de menú superior (en teléfonos[71]), permiten conocer más detalles sobre el interfaz Wi-Fi. Por ejemplo, si las ondas Wi-Fi aparecen en color blanco indica que se dispone de conectividad completa a Internet, mientras que si aparecen de color naranja, indica que algunos servicios (de Google) pueden no estar disponibles [Ref.- 24][Ref.- 25] [72].

733. El estado del interfaz Wi-Fi no puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado o menú. Desafortunadamente, la barra superior de estado no proporciona información sobre el estado del interfaz Wi-Fi, no siendo posible saber si el mismo está activo o no, salvo que el dispositivo móvil esté conectado a una red Wi-Fi actualmente:

734. Únicamente desde los ajustes rápidos, o desde el menú de "Ajustes" (pero éste no permite un acceso sencillo, ágil y rápido), es posible ver el estado actual del interfaz Wi-Fi: "Wi-Fi" (indica que el interfaz Wi-Fi está activado, aunque no esté conectado a ninguna red actualmente) o "Wi-Fi Desactivado".

[71] En tabletas es suficiente con desplazar con un dedo la barra de menú superior, en concreto desde la esquina superior derecha, para acceder a los ajustes rápidos.

[72] En algunas versiones de Android, la existencia de flechas hacia arriba y hacia abajo indican que el dispositivo móvil está transmitiendo o recibiendo datos, respectivamente.



735. Android mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil, es decir, si el interfaz Wi-Fi estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo, incluso con el terminal bloqueado.

736. Igualmente, al salir del modo avión el estado del interfaz Wi-Fi será restaurado, activándose de nuevo en el caso de haber estado activo previamente (antes de activar el modo avión).

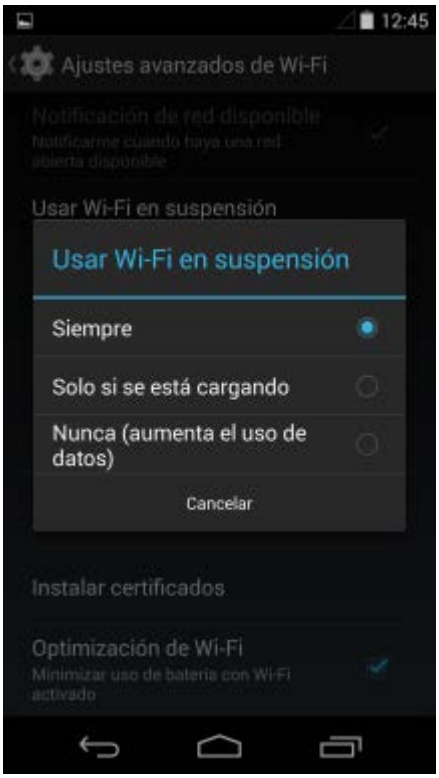
737. Cuando el dispositivo móvil está conectado a una red, el interfaz Wi-Fi permanece activo tras pasar al estado de espera o *stand-by* (desatendido), es decir, el dispositivo móvil está encendido pero con la pantalla apagada y bloqueado (ver posteriormente la opción de configuración asociada), y sigue generando tráfico periódicamente.

738. En caso de no estar conectado a una red Wi-Fi, en el estado de espera (o suspendido) el dispositivo móvil genera por defecto el tráfico 802.11 asociado a las tramas de verificación de disponibilidad de redes Wi-Fi (*probe request*).

Nota: cada 10 segundos, por defecto inicialmente (siendo posteriormente este intervalo mayor, de unos 16,4 segundos aproximadamente, en ocasiones superándose este valor; por ejemplo, 20 segundos), el dispositivo móvil genera tramas *probe request* de tipo *broadcast* para verificar la disponibilidad de redes Wi-Fi en su zona de alcance.

739. El comportamiento del interfaz Wi-Fi respecto a las operaciones de ahorro de energía del dispositivo móvil puede ser configurado desde el menú "Ajustes - Wi-Fi - Ajustes avanzados", a través de las siguientes opciones:

740. La opción "Usar Wi-Fi en suspensión" permite acceder a las diferentes alternativas de configuración disponibles: "Siempre" (opción por defecto), "Sólo si se está cargando", o "Nunca (aumenta el uso de datos)":



741. La primera opción permite que el interfaz Wi-Fi esté activo y sea utilizado siempre, incluso cuando el dispositivo móvil está suspendido. La segunda opción permite el uso de Wi-Fi si el dispositivo móvil está suspendido sólo si está conectado a la electricidad (cargando), y la tercera opción nunca hace uso de Wi-Fi si el dispositivo móvil está

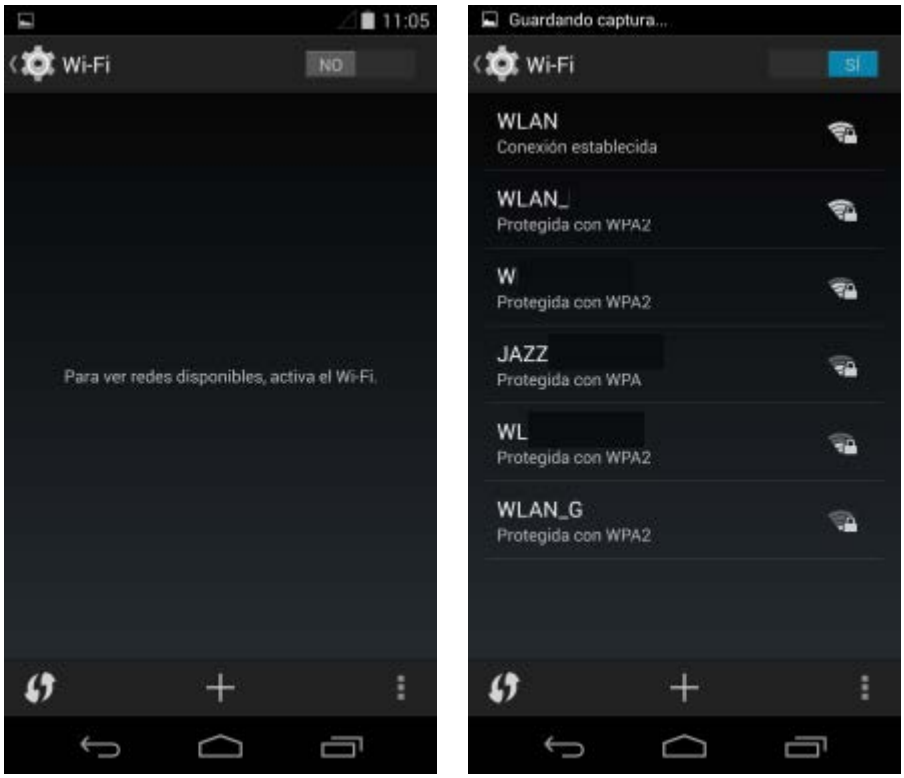
suspendido, por lo que en ese caso se hará uso de la conexión de datos de telefonía móvil (aumentando potencialmente el consumo de datos).

742. La opción "Optimización de Wi-Fi" (activa por defecto) indica que se intente minimizar el consumo de batería cuando el interfaz Wi-Fi está activado.

743. Una vez deshabilitado el interfaz Wi-Fi se hará uso de las capacidades de datos de telefonía móvil (ver apartado "5.14.2. Selección de la red de datos en Android").

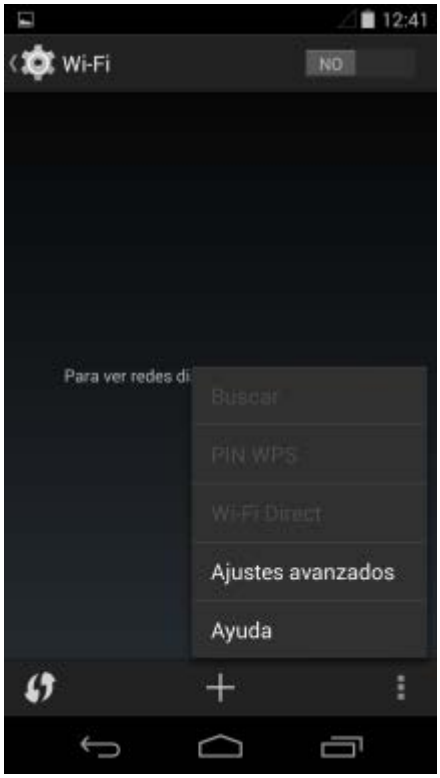
744. La configuración detallada de las redes Wi-Fi puede llevarse a cabo a través del menú "Ajustes - Wi-Fi - Ajustes avanzados". Adicionalmente a los ajustes ya mencionados, la opción "Solo conexiones estables" permite hacer uso de redes Wi-Fi si tienen buena conexión a Internet. Por otro lado, la opción "Banda de frecuencia Wi-Fi" permite seleccionar entre una configuración automática (por defecto) o manual, eligiendo sólo la banda de 2,4Ghz o sólo la de 5Ghz. Estas opciones no tienen implicaciones desde el punto de vista de seguridad.

745. Debe tenerse en cuenta que, al igual que para el interfaz Bluetooth, para poder llevar a cabo la configuración completa de la pila de comunicaciones Wi-Fi a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:



746. Por ejemplo, la funcionalidad asociada a la opción para añadir una red Wi-Fi manualmente, "+" (signo más) no está disponible (o habilitada) hasta que el interfaz Wi-Fi no ha sido activado.

747. Sin embargo, en el caso de Wi-Fi, algunos ajustes de configuración avanzados sí están disponibles incluso con el interfaz Wi-Fi desactivado, como por ejemplo los siguientes:



748. La dirección del interfaz Wi-Fi está disponible a través del menú "Ajustes - Información del teléfono - Estado", y en concreto, en el campo "Dirección MAC de Wi-Fi". La dirección es visible tanto si el interfaz Wi-Fi se encuentra activo como si está desactivado:

Nota: la parte de la dirección Wi-Fi asociada al fabricante (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor

"64:89:9a" está asignado por el IEEE (http://standards.ieee.org/regauth/oui/index.shtml) a "LG":

```
  64-89-9A   (hex)            LG Electronics
  64899A     (base 16)        LG Electronics
                              60-39, Gasan-dong, Geumcheon-gu
                              Seoul Seoul 153-801
                              KOREA, REPUBLIC OF
```

749. Es aconsejable comparar la dirección Wi-Fi del dispositivo móvil con su dirección Bluetooth (ver apartado "5.13. Comunicaciones Bluetooth"), con el objetivo de identificar si se trata de direcciones correlativas. En caso afirmativo, un potencial atacante podría obtener la dirección de Bluetooth a partir de la dirección Wi-Fi, con los riesgos que ello conlleva [Ref.- 1], al emplearse la ocultación de la dirección Bluetooth en diferentes escenarios como mecanismo de seguridad.

750. En el caso del dispositivo móvil empleado para la elaboración de la presente guía ambas direcciones comparten el mismo rango del fabricante, pero sin ningún otro elemento común (asignación aleatoria dentro de ese rango).

5.14.2 SELECCIÓN DE LA RED DE DATOS EN ANDROID

Nota: la selección de la red de datos en Android afecta principalmente a la red de datos de telefonía móvil 2/3/4G (analizada en el apartado "5.16. Comunicaciones móviles: voz y datos") y al interfaz Wi-Fi (ver el presente apartado).

751. Debido a las múltiples opciones de conectividad de datos disponibles en los dispositivos móviles, como Bluetooth, y principalmente Wi-Fi y 2/3/4G, en caso de haber múltiples opciones habilitadas y disponibles, Android gestiona cual es la mejor conexión de datos a usar en cada momento a través del servicio Connectivity Service (o Connectivity Manager) [Ref.- 52]. De esta forma evita que el usuario tenga que decidir constantemente que conexión utilizar y proporciona la conectividad necesaria a las apps que ejecutan en el dispositivo móvil.

752. El Connectivity Service emplea diferentes criterios para seleccionar y mantener la mejor y única opción de conexión de datos, que por defecto da prioridad al interfaz Wi-Fi frente al interfaz de telefonía móvil (2/3/4G):

- Si Wi-Fi está activo y se activa 2/3/4G, este segundo no llegará a ser utilizado.
- Si 2/3/4G está activo y se activa Wi-Fi, la conexión 2/3/4G dejará de ser utilizada.
- Si Wi-Fi está activo y se desactiva, el servicio comprobará el estado y la configuración de 2/3/4G, y si está disponible, lo habilitará y hará uso de este interfaz de red.

753. Los eventos de activación y desactivación de los dos interfaces, Wi-Fi y 2/3/4G, pueden ser visualizados a través de los iconos del menú superior de Android.

754. El comportamiento del interfaz Wi-Fi, y en consecuencia del interfaz 2/3/4G, respecto a las operaciones de ahorro de energía del dispositivo móvil, cuando éste se encuentra en estado suspendido, puede ser configurado desde el menú de ajustes de Wi-Fi, tal y como se detalla en el apartado "5.14.1. Utilización y configuración de las comunicaciones Wi-Fi".

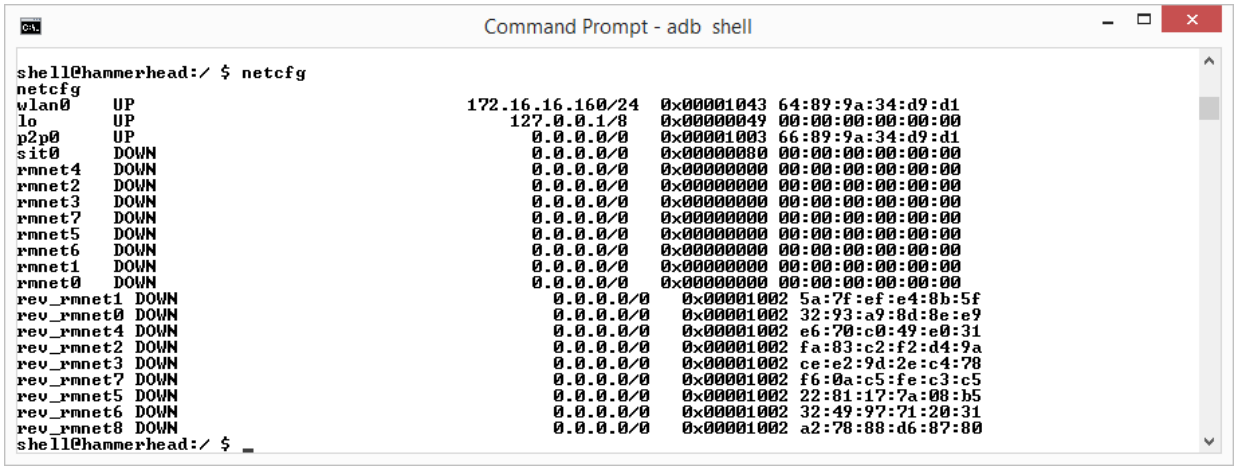
755. El Connectivity Service no permite disponer de varias conexiones activas simultáneamente, opción recomendada desde el punto de vista de seguridad para evitar escenarios *dual homing* donde la conexión Wi-Fi y la conexión de datos de telefonía móvil

(2/3/4G) están activas simultáneamente, con el objetivo de que el dispositivo móvil no actúe de pasarela entre distintas redes.

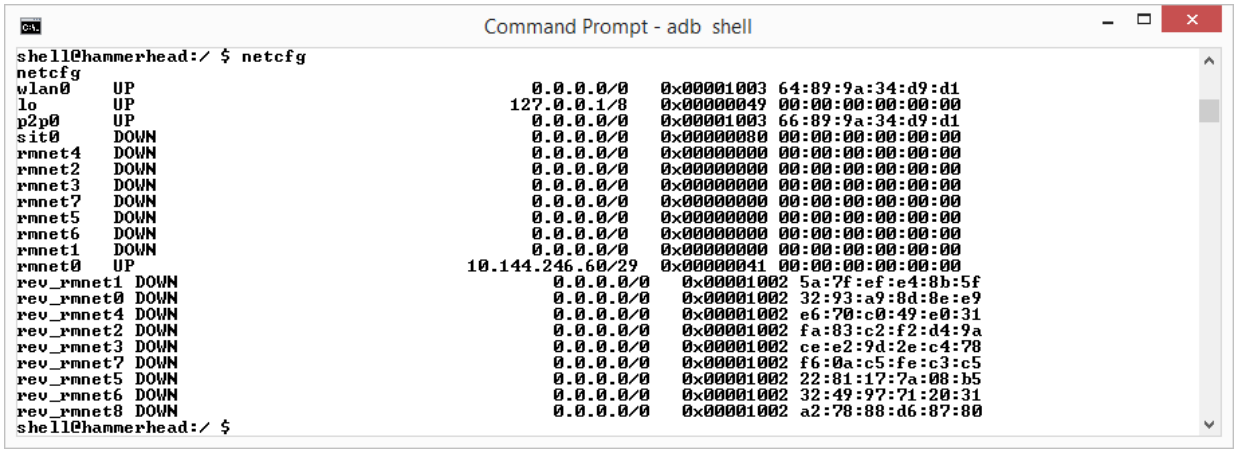
756. Desde el punto de vista de seguridad podría considerarse más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil (cuando estén disponibles según la cobertura existente) en lugar de a través de redes Wi-Fi (especialmente si se quiere hacer uso de redes abiertas, opción desaconsejada desde el punto de vista de seguridad), siempre que se fuerce a que la conexión de datos de telefonía móvil empleé tecnologías 3/4G frente a 2G (ver apartado "5.16. Comunicaciones móviles: voz y datos"). Para ello sería necesario deshabilitar el interfaz Wi-Fi y habilitar las comunicaciones móviles de datos.

757. En el caso contrario, en el que se quiera cursar todo el tráfico de datos a través de redes Wi-Fi (con un nivel de seguridad adecuado) se recomienda consultar el apartado "5.16. Comunicaciones móviles: voz y datos", que contiene información detallada de cómo deshabilitar el interfaz de datos de telefonía móvil 2/3/4G.

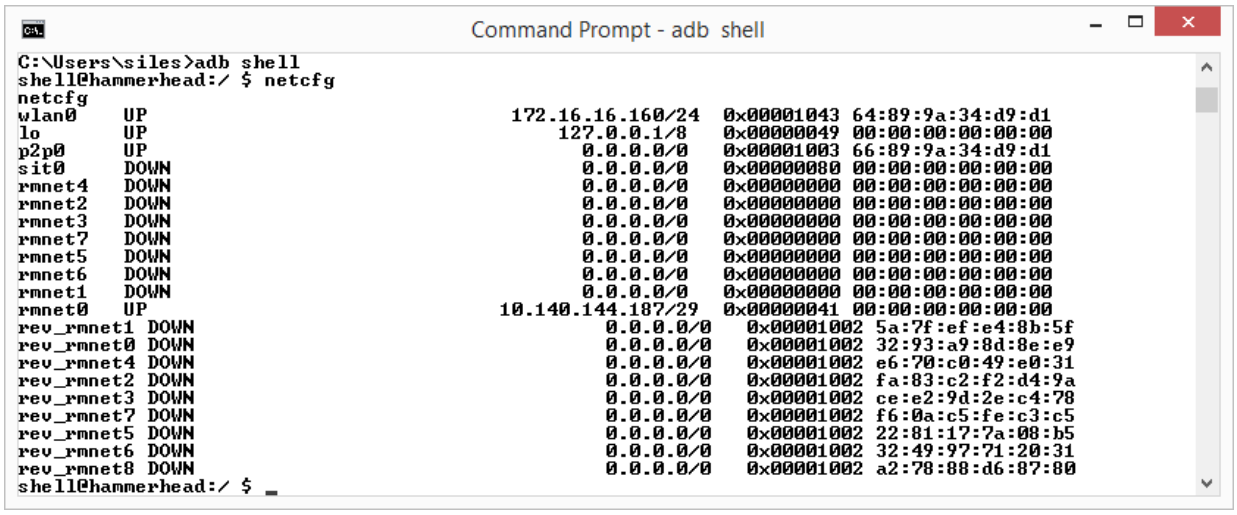
758. Cuando ambas conexiones de datos han sido activadas, pese a que a través del comando "netcfg" (vía "adb shell") es posible ver la asignación de direcciones IP en ambas redes, Android únicamente utilizará la red de mayor prioridad. En la imagen inferior es posible identificar como el interfaz de la red de telefonía móvil ("rmnet0") se encuentra en estado DOWN al estar activo el interfaz Wi-Fi ("wlan0"). Normalmente la dirección IP mostrada para el interfaz no activo, "rmnet0" en este ejemplo, tiene el valor 0.0.0.0:



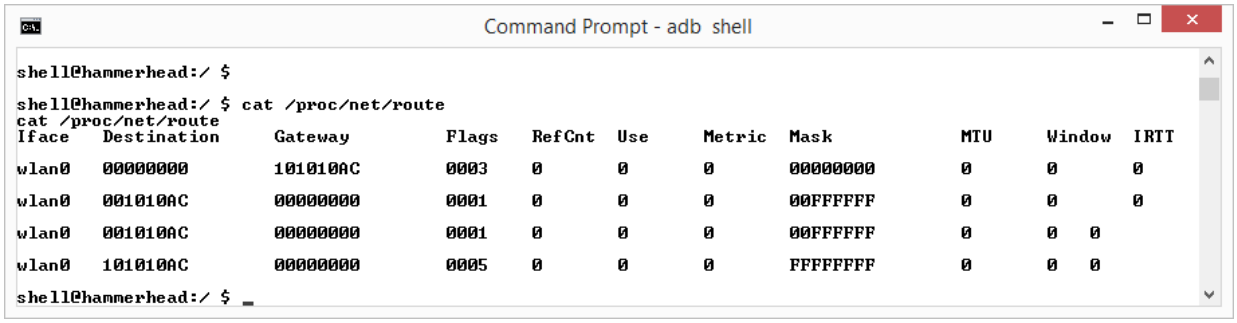
759. En el caso del interfaz Wi-Fi ("wlan0"), pese a ser deshabilitado, sigue en estado "UP", pero con la dirección IP 0.0.0.0, empleándose en este caso el interfaz de telefonía móvil:



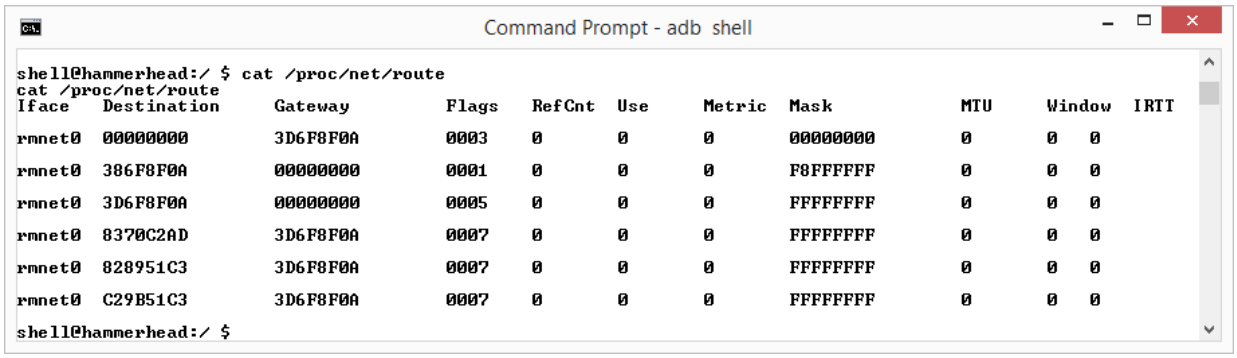
760. En algunos escenarios, como por ejemplo tras el arranque inicial del dispositivo móvil, ambos interfaces de datos pueden estar activos ("UP"). En la imagen inferior no es posible identificar el interfaz empleado, ya que tanto el interfaz de la red de telefonía móvil ("rmnet0") como el interfaz Wi-Fi ("wlan0") se encuentran en estado UP al estar habilitados los dos. Cada uno de ellos muestra la dirección IP correspondiente a la asignación de DHCP recibida desde la red de telefonía móvil y Wi-Fi, respectivamente:



761. Sin embargo, a través de la tabla de rutas ("/proc/net/route") es posible validar el comportamiento descrito y el interfaz de datos prioritario. La imagen inferior muestra como el tráfico es dirigido a través del interfaz Wi-Fi ("wlan0") pese a estar ambos interfaces de red activos, empleando el router por defecto 172.16.16.16 (en hexadecimal, y con los valores invertidos, 0x101010AC):



762. Posteriormente, una vez se ha deshabilitado el interfaz Wi-Fi, el tráfico se envía a través del interfaz 2/3/4G ("rmnet0"), empleando el router 10.143.111.61 (en hexadecimal, y con los valores invertidos, 0x3D6F8F0A):



5.14.3 RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI

763. Este apartado proporciona recomendaciones de configuración a través de los diferentes parámetros y opciones disponibles en Android para la conexión segura a redes Wi-Fi.

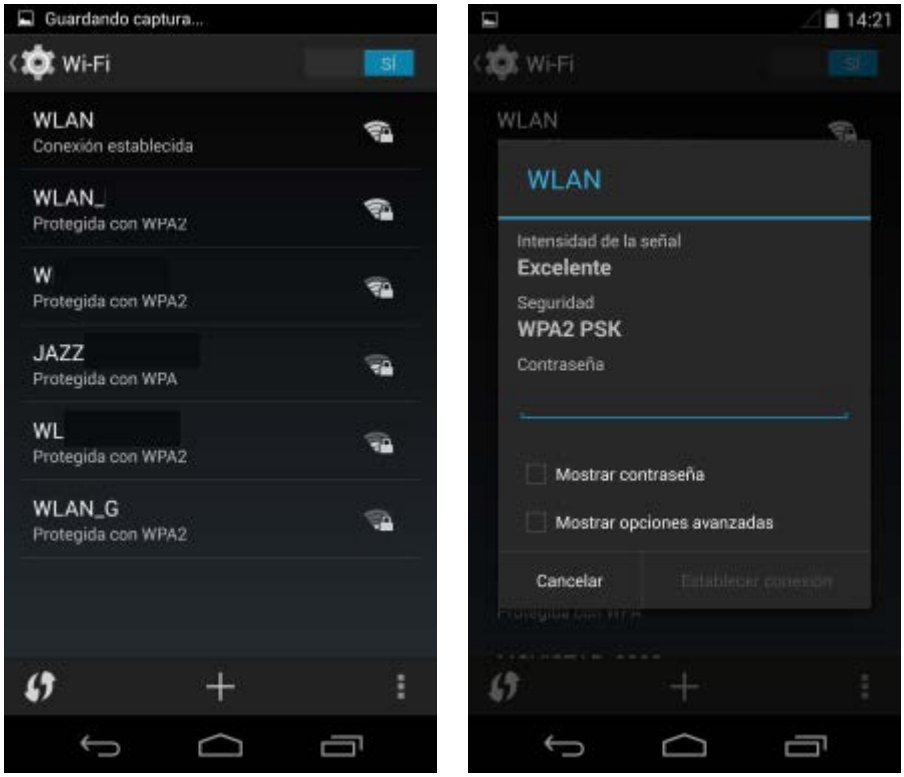
764. La configuración manual y detallada de las redes Wi-Fi se puede realizar desde el menú "Ajustes - Wi-Fi", y en concreto mediante la opción de añadir una red Wi-Fi manualmente, a través del botón "+" (signo más) de la parte inferior. Esta opción permite seleccionar todas las opciones de configuración de conexión de una nueva red Wi-Fi, incluyendo el nombre de red (o SSID), el mecanismo de seguridad a emplear (abierta o ninguna, WEP, WPA/WPA2 PSK o 802.1x EAP), etc (todos ellos analizados posteriormente). La opción "Mostrar opciones avanzadas" permite seleccionar el proxy y la configuración de la dirección IP:

765. Adicionalmente, mediante la selección de una de las redes disponibles al alcance del dispositivo móvil (listadas en la misma pantalla bajo la sección "Wi-Fi") es posible seleccionar la red Wi-Fi con la que se desea establecer la conexión.

766. Como se explicará posteriormente en detalle, desde el punto de vista de seguridad se recomienda seleccionar la red Wi-Fi con la que se quiere establecer la conexión de la lista de redes visibles, en lugar de añadirla manualmente a través del botón "+".

767. Habitualmente se recomendaba hacer uso del mecanismo de configuración manual frente a seleccionar la red Wi-Fi desde el listado de redes disponibles, ya que en este segundo caso, no se dispone de tanta flexibilidad y granularidad para seleccionar los diferentes parámetros de configuración y los mecanismos de seguridad de la red. Sin embargo, en el caso de Android se recomienda añadir la red Wi-Fi desde el listado de redes disponibles (ver apartado "5.14.5. Conexión automática a redes Wi-Fi: ocultas o visibles") para evitar una vulnerabilidad existente al añadir la red Wi-Fi de forma manual.

768. Las redes aparecen clasificadas en la lista (por defecto) en orden según la intensidad de señal de cada una de ellas, siendo las redes de la zona superior las de mayor intensidad de señal (de mayor a menor intensidad). La lista permite identificar los mecanismos de seguridad empleados por cada una de la redes Wi-Fi bajo el nombre de cada red:



769. Para establecer la conexión con una red próxima únicamente es necesario introducir la contraseña de acceso a la red (ver imagen superior derecha) en caso de estar protegida por una contraseña (WEP o WPA/WPA2 PSK). En el caso de redes abiertas directamente se establece la conexión con la red una vez ha sido seleccionada por parte del usuario de la lista (o una vez se ha proporcionado su nombre si se añadiera manualmente):

770. Todas las redes que implementan algún tipo de mecanismo de seguridad, WEP, WPA ó WPA2, aparecen con un candado en el icono de la red, pero Android adicionalmente permite diferenciar el mecanismo de seguridad empleado específicamente desde el listado de redes disponibles, proporcionando los detalles bajo el nombre de la red, y permitiendo diferencir por ejemplo entres redes WPA y WPA2.

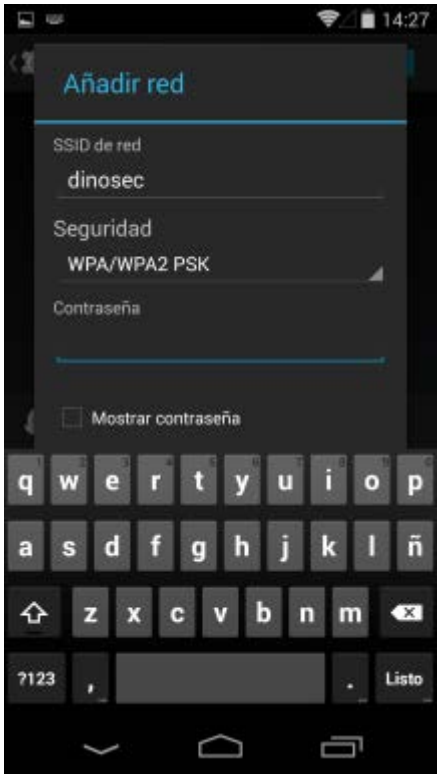
771. Al establecer una primera conexión con una nueva red Wi-Fi, se recomienda agregar la nueva red Wi-Fi de forma automática a través del listado de redes disponibles (debido a una vulnerabilidad al añadirla manualmente descrita posteriormente), pese a que no sea posible visualizar y especificar todas las opciones de configuración disponibles, descritas a continuación.

772. El proceso de configuración de la contraseña puede permitir al usuario no ocultar el texto introducido en pantalla (por ejemplo con el carácter "·") mediante la opción "Mostrar contraseña" (no habilitada por defecto).

773. En caso de habilitar esta funcionalidad, opción no recomendada desde el punto de vista de seguridad, el usuario debe prestar atención a cómo y dónde introduce la contraseña de conexión a la red Wi-Fi para evitar que un potencial atacante la obtenga mediante acceso visual a la pantalla del dispositivo móvil.

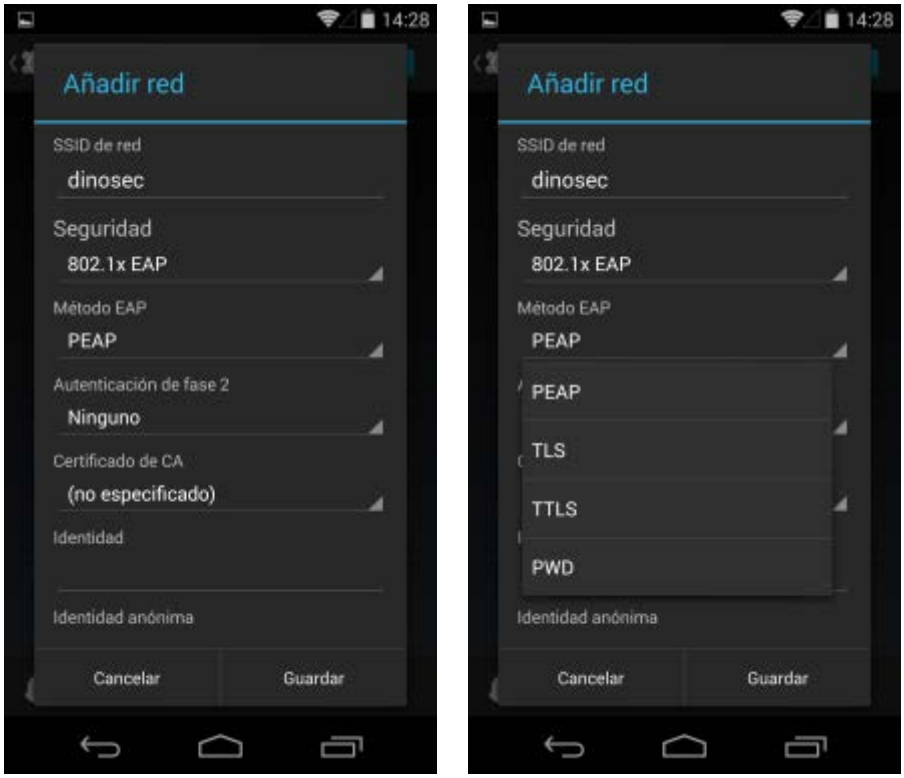
774. Dentro de las opciones de configuración de una nueva red Wi-Fi, la primera pantalla de configuración hace posible especificar el nombre de la red (SSID) y el mecanismo de seguridad a emplear: Ninguna (opción por defecto), WEP, WPA/WPA2 PSK o 802.1x EAP.

775. En caso de seleccionar una red WEP o WPA/WPA2 PSK, es necesario especificar la contraseña de la red:



776. En el caso de seleccionar una red 802.1x EAP, es necesario especificar el tipo de EAP a emplear, PEAP, TLS, TTLS o PWD[73] y el método de autentificación de fase 2, junto a los certificados asociados (opcionalmente) y a las credenciales del usuario (descritos posteriormente):

[73] Los tres últimos tipos de métodos EAP corresponden según los estándares a EAP-TLS, EAP-TTLS y EAP-PWD.



777. Desafortunadamente, Android no permite especificar detalladamente los mecanismos de autentificación y de cifrado de datos, no siendo posible diferenciar entre redes WPA y redes WPA2 (tanto Personal, PSK, como Empresarial, o Enterprise), ni el tipo de cifrado: TKIP, AES o ambos.

778. Por otro lado, tampoco es posible especificar si se permiten conexiones a redes con infraestructura, es decir, puntos de acceso, a redes entre equipos o ad-hoc, o ambas.

779. Android por defecto sigue sin permitir conexiones Wi-Fi ad-hoc (IBSS, Independent Basic Service Set), permitiendo únicamente conexiones a redes Wi-Fi con infraestructura, es decir, basadas en puntos de acceso. La pantalla que muestra el listado de redes Wi-Fi disponibles directamente no muestra las redes ad-hoc.

Nota: esta limitación del gestor de conexiones Wi-Fi de Android está implícita en el diseño del sistema y es conocida desde las primeras versiones de Android [Ref.- 40].

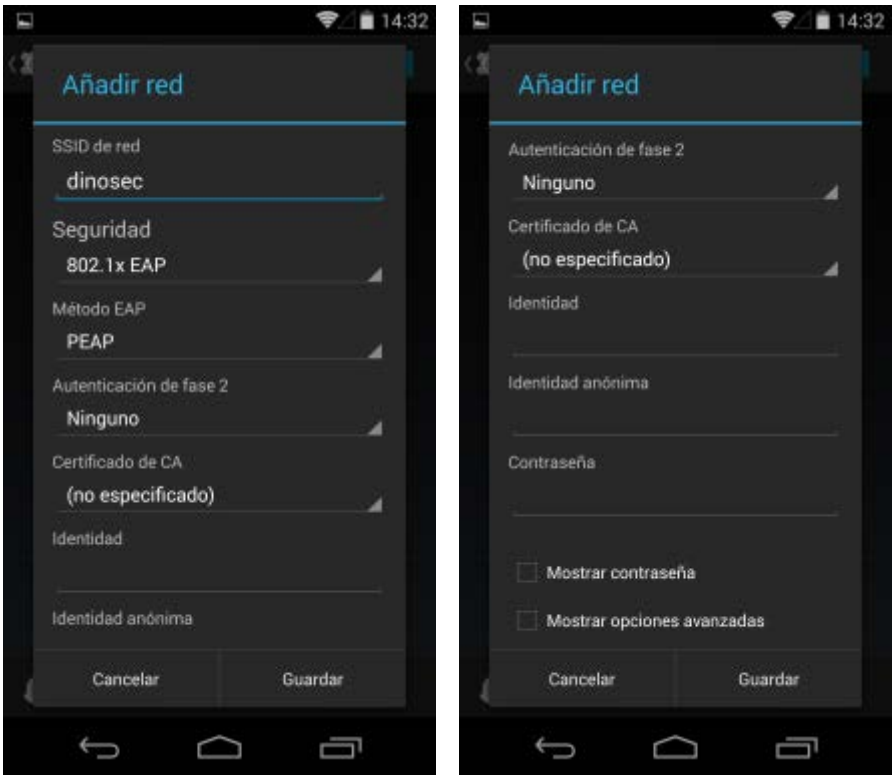
Aunque desde el punto de vista de seguridad es preferible conectar a redes Wi-Fi con infraestructura, dado que hoy en día es también posible hacer uso de redes ad-hoc con un nivel de seguridad razonable, existe la posibilidad de modificar este comportamiento existente por defecto y habilitar el soporte para redes *ad-hoc* en dispositivos móviles Android *rooted* a través de un conjunto de parches y modificaciones disponibles, por ejemplo, en distribuciones de Android de terceros, como CyanogenMod [Ref.- 41].

La versiones 2.3, 4.0 (y posteriores) de Android implementan soporte para Wi-Fi Direct ("P2P", ver apartado "5.14.7. Wi-Fi Direct ("P2P")"), un estándar de comunicación Wi-Fi directa entre dispositivos que es similar (pero no sustituye completamente) a las comunicaciones *ad-hoc* [Ref.- 42], y añade mejoras de seguridad, facilidad de configuración, rendimiento y consumo.

780. Igualmente, el proceso de configuración de las redes Wi-Fi en Android no permite claramente, y de forma explícita, especificar o comprobar si la red Wi-Fi es oculta o visible (ver apartado "5.14.5. Conexión automática a redes Wi-Fi: ocultas o visibles").

781. Se recomienda conectarse únicamente a redes que emplean WPA2 (Personal, WPA2-PSK, o Enterprise, WPA2) como mecanismo de autentificación, y AES como mecanismo de cifrado. En su defecto, debería emplearse WPA/TKIP (desaconsejado actualmente), pero en ningún caso se debe hacer uso de WEP.

782. En caso de emplear WPA2 (o WPA) en su versión Enterprise, es decir, con mecanismos basados en 802.1X/EAP, la pantalla de ajustes permite especificar los parámetros de configuración asociados al tipo de mecanismo EAP empleado:



783. Todos los campos posibles de configuración están disponibles en el interfaz de usuario de Android para los distintos tipos de EAP, lo que puede crear cierta confusión, ya que no todos los tipos de EAP hacen uso de todos y cada uno de los diferentes campos mostrados.

784. Una vez seleccionado el tipo de método EAP a emplear, en primer lugar es necesario definir el tipo de autentificación interna (o de fase 2): Ninguno, MSCHAPV2 (PEAPv0) o GTC (EAP-GTC, Generic Token Card).

785. Adicionalmente, para PEAP (Protected EAP) debe definirse el certificado digital raíz de la autoridad certificadora (CA) que ha emitido el certificado digital del servidor de autentificación de la red Wi-Fi (RADIUS), mediante el campo "Certificado de CA", que debe haber sido añadido previamente al dispositivo móvil (ver apartado "5.7.3. Añadiendo certificados digitales"). Asimismo, deben proporcionarse las credenciales del usuario (nombre de usuario y contraseña, y opcionalmente el dominio Windows (por ejemplo "DOMINIO\usuario") en los campos "Identidad" y "Contraseña" (ver imágenes superiores).

786. Por otro lado, para TTLS (conocido como EAP-TTLS) es necesario definir los mismos elementos que para PEAP, pero haciendo uso de la identidad anónima a utilizar para la autentificación externa o de fase 1, mediante el campo "Identidad anónima" (por ejemplo, con el valor estándar "anonymous").

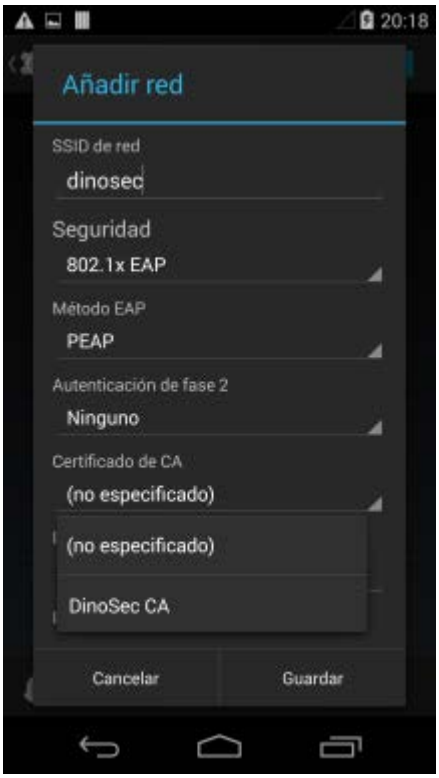
787. Por último, para TLS (conocido como EAP-TLS) es necesario definir los mismos elementos que para PEAP, pero sustituyendo las credenciales tradicionales del usuario (nombre de usuario y contraseña) por un certificado digital cliente personal y que identifica al usuario, mediante el campo "Certificado de usuario", y que también debe haber sido añadido previamente al dispositivo móvil (ver apartado "5.7.3. Añadiendo certificados digitales").

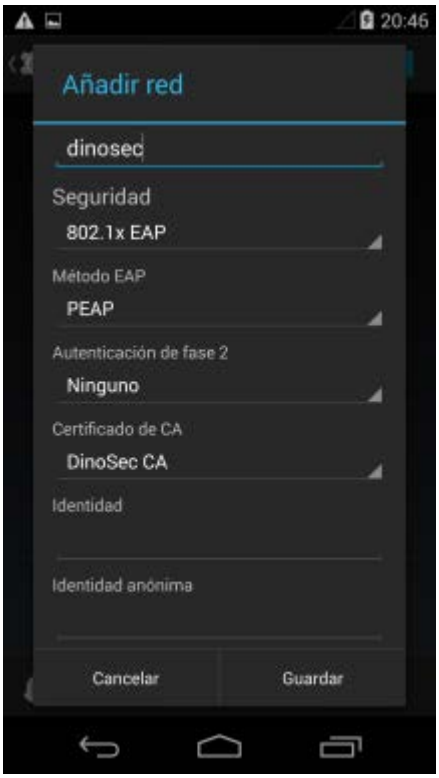
788. Tanto en el caso de autentificación PEAP como TLS o TTLS, es necesario (aunque opcional) importar previamente en Android el certificado digital de la autoridad certificadora (CA), raíz o intermedia, empleada para generar los certificados digitales asociados al servidor de autentificación de la red Wi-Fi (servidor RADIUS).

789. Incluso en el caso en el que se usen certificados emitidos por una de las CAs públicas ya existentes por defecto en Android, éstas no son mostradas por defecto en el campo "Certificado de CA", por lo que también es necesario importarlas manualmente, especificando que su propósito es utilizarlas para redes Wi-Fi.

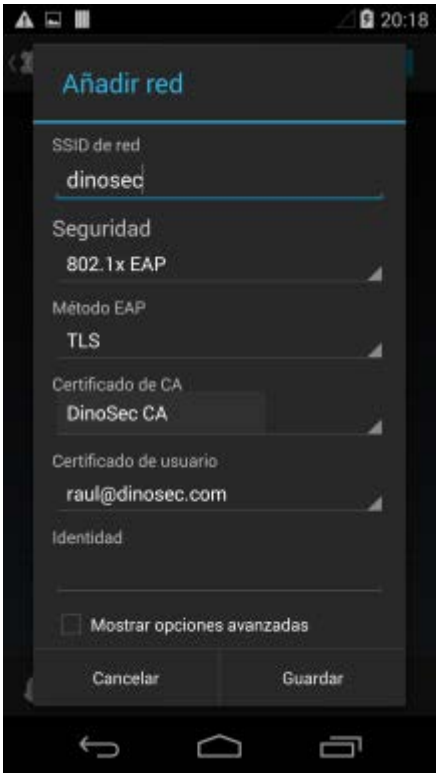
790. Para instalar el certificado basta con transferir el fichero del certificado digital al dispositivo móvil, a través de un servidor web (preferiblemente propio, frente a servidores públicos de terceros [Ref.- 46]), correo electrónico, o mediante una tarjeta de almacenamiento externa, o el almacenamiento interno del propio dispositivo móvil (ver apartado "5.7.3. Añadiendo certificados digitales").

791. Una vez el certificado ha sido importado en el dispositivo móvil, estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en PEAP, TTLS o TLS, desde el campo "Certificado de CA":





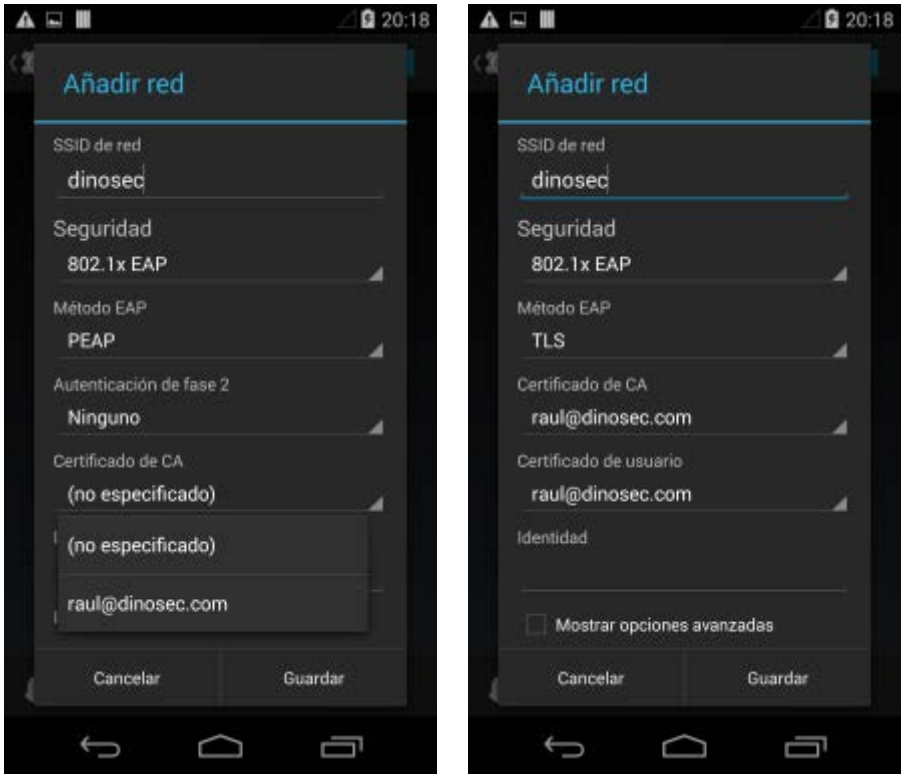
792. En el caso de emplear EAP-TLS siempre es necesario importar el certificado digital personal del cliente (en formato PKCS#12) en el dispositivo móvil. Para instalar el certificado personal basta con transferir el fichero del certificado digital personal (".pfx" o ".p12") al dispositivo móvil, por ejemplo, a través de una tarjeta de almacenamiento externa, , o el almacenamiento interno del propio dispositivo móvil, un correo electrónico, o desde la web.



793. Igualmente, una vez el certificado personal ha sido importado en el dispositivo móvil (ver apartado "5.7.3. Añadiendo certificados digitales"), estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en TLS, desde el campo "Certificado de usuario" (ver imágnes superiores).

Nota: el certificado digital cliente (o de usuario) es identificado por defecto con un *string* con letras y números, correspondientes al identificador de la clave, si no se modificó su nombre asociado durante el proceso de importación (ver apartado "5.7.3. Añadiendo certificados digitales"). En caso de que se modificase su nombre, el certificado es mostrado con el nombre elegido por el usuario. Android permite importar el mismo certificado digital cliente con diferentes nombres múltiples veces.

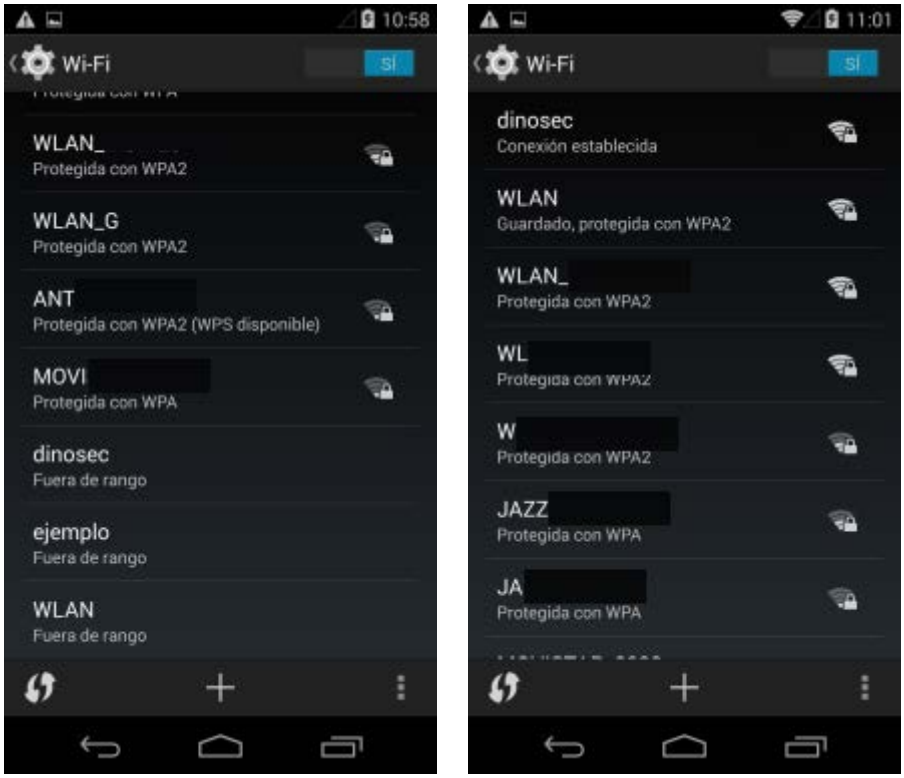
794. El certificado de la CA puede ser importado simultáneamente junto con el certificado digital cliente empleado para EAP TLS (en este caso, ambos certificados, tanto el cliente como el de la CA, son identificados con el mismo nombre), o de manera independiente (tal como se describió previamente):



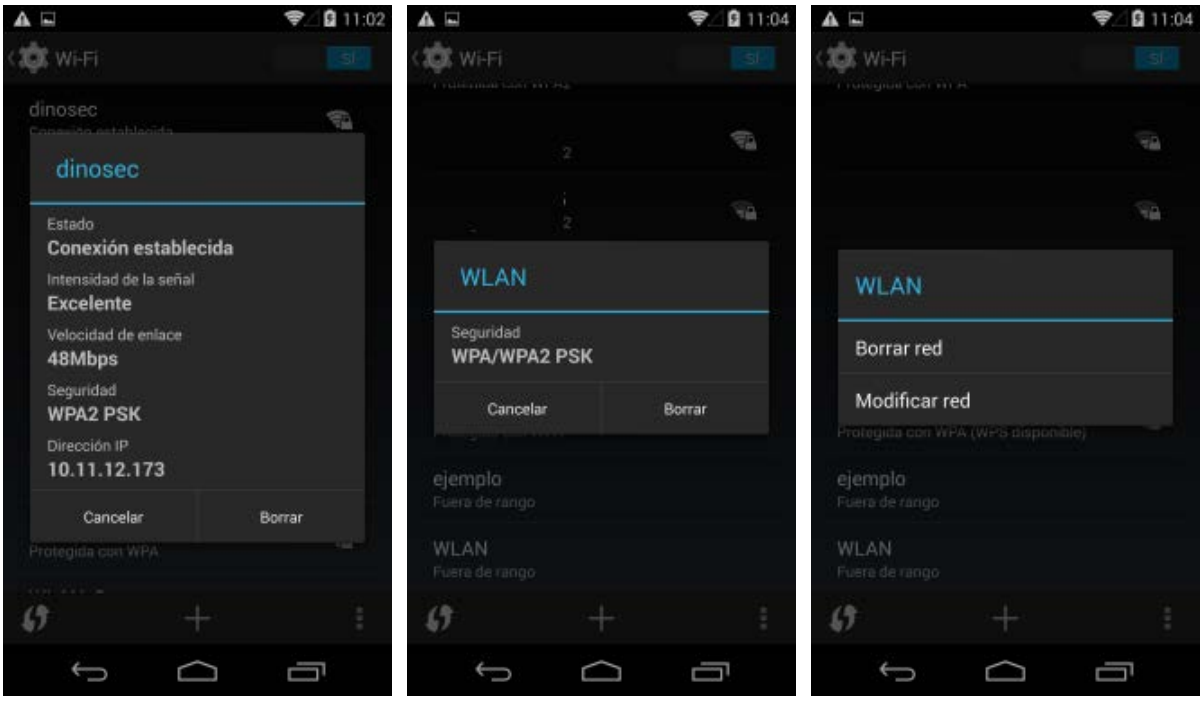
5.14.4 LISTA DE REDES PREFERIDAS (PNL)

795. La lista de redes preferidas (PNL, Preferred Network List), es decir, a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo (ver apartado "5.14.5. Conexión automática a redes Wi-Fi: ocultas o visibles"), puede ser visualizada tras habilitar el interfaz Wi-Fi, desde el menú "Ajustes - Wi-Fi", y en concreto, al final de la lista de redes disponibles actualmente. Las redes almacenadas en la PNL son identificadas con el texto "Fuera de rango" (por ejemplo, las redes Wi-Fi "dinosec", "ejemplo" y "WLAN" en la imagen inferior izquierda).

796. Las redes existentes en la PNL que están disponibles actualmente (suponiendo que el dispositivo móvil está conectado a otra red conocida, por ejemplo a la red Wi-Fi "dinosec") aparecerán en la lista de redes disponibles con un distintivo que las identifica como redes con las que previamente se ha establecido una conexión, mediante por ejemplo el texto "Guardado" (por ejemplo, la red "WLAN" en la imagen inferior derecha), salvo que se trate de la red Wi-Fi a la que está actualmente conectado el dispositivo móvil, ya que ésta aparecerá con el texto "Conexión establecida":



797. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación breve sobre la misma), es posible eliminarla de la PNL a través del botón "Borrar" (tanto si es visible actualmente y hay establecida una conexión con ella, imagen izquierda, como si es visible pero no hay una conexión establecida, imagen central, o como si no es visible actualmente pero está en la PNL, imagen derecha):

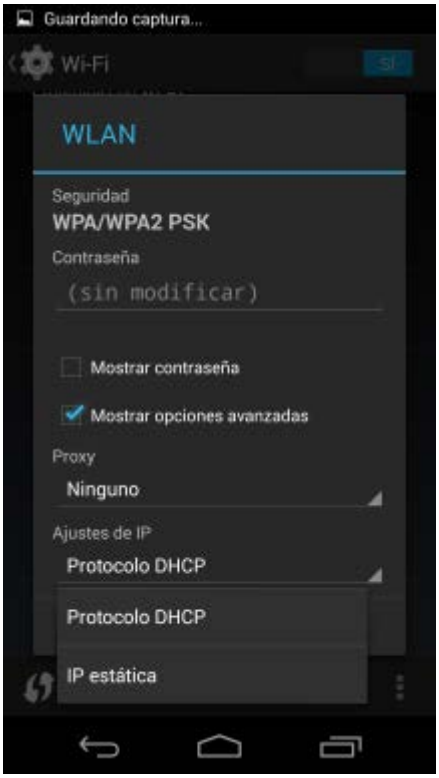


798. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación prolongada sobre la misma), es también posible eliminarla de la PNL a través de la opción "Borrar red" o editar sus detalles (como la contraseña de

acceso) a través de la opción "Modificar red" (tanto si no es visible actualmente, como si lo es - ver imagen superior derecha):

799. Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP dinámica obtenida mediante el protocolo DHCP (ver apartado "5.17. Comunicaciones TCP/IP").

800. Android permite, a través de la opción "Mostrar opciones avanzadas", fijar una dirección IP estática (junto a la puerta de enlace, la máscara o prefijo de red, y los servidores DNS primario y secundario):



801. Para llevar a cabo la configuración de TCP/IP, o modificaciones en la misma, sí es necesario que el interfaz Wi-Fi esté activo para poder seleccionar la red Wi-Fi de la lista de redes visibles o de la PNL.

802. La PNL también está disponible indirectamente a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Uso de datos - [...] - Puntos de acceso móviles", con el objetivo de poder definir qué puntos de acceso Wi-Fi son móviles (de entre las redes Wi-Fi conocidas) y tienen asociado un consumo de datos:

803. En resumen, desde el punto de vista de seguridad de Android como cliente Wi-Fi, se recomienda hacer uso de redes inalámbricas no ocultas (ver apartado "5.14.5. Conexión automática a redes Wi-Fi: ocultas o visibles"), basadas en WPA2 con cifrado AES, y autentificación de tipo Personal, con una contraseña de acceso (PSK, Personal Shared Key) suficientemente robusta (más de 20 caracteres), o autentificación de tipo Enterprise, basada en mecanismos de autentificación 802.1X/EAP, y empleando EAP-TLS (con certificados digitales cliente) preferiblemente, y correctamente configurada y gestionada.

Nota: con el objetivo de proteger el dispositivo móvil y aumentar su nivel de seguridad, se desaconseja el uso de redes inalámbricas públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autentificación y cifrado), como por ejemplo *hotspots* Wi-Fi disponibles en hoteles, aeropuertos o centros de conferencias [Ref.- 1].

Los riesgos de seguridad asociados a este tipo de entornos incluyen la captura e interceptación del tráfico y datos por parte de un potencial atacante, la posibilidad de inyección de tráfico para la realización de ataques directos y de accesos no autorizados contra el dispositivo móvil, ataques de suplantación de la red, y ataques de denegación de servicio (DoS), entre otros.

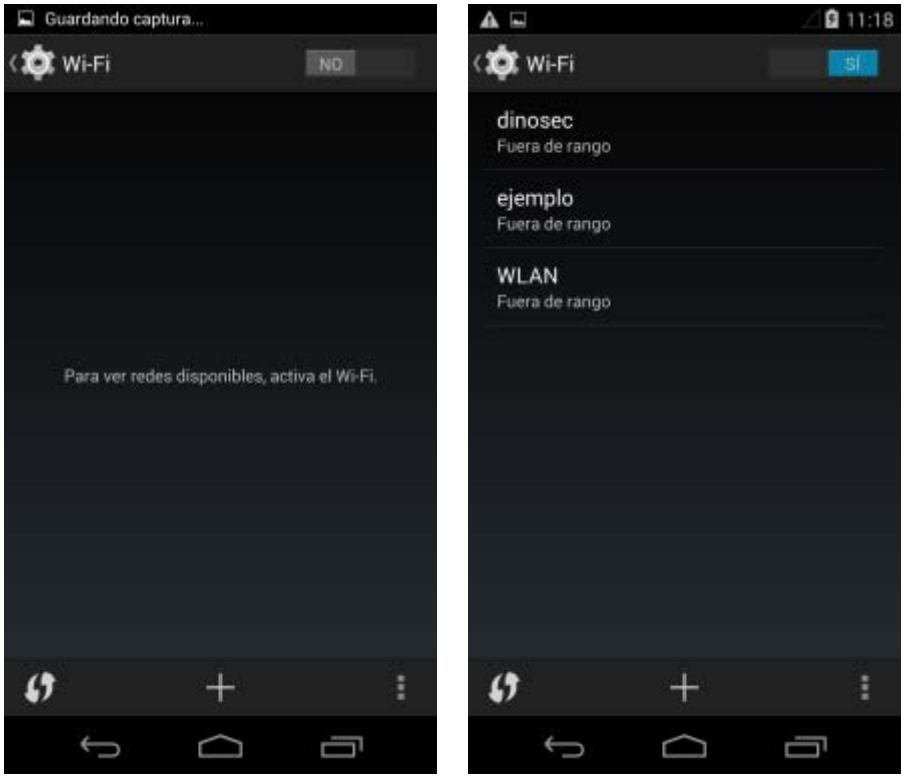
5.14.5 CONEXIÓN AUTOMÁTICA A REDES WI-FI: OCULTAS O VISIBLES

804. Android intenta conectarse automáticamente a las redes Wi-Fi existentes en su lista de redes preferidas (PNL, Preferred Network List). Si alguna de estas redes Wi-Fi está disponible, establecerá la conexión automáticamente.

Nota: no se ha identificado ninguna opción de configuración en el interfaz de usuario de Android para deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi se encuentra activo. De ahí la importancia de deshabilitar el interfaz Wi-Fi si no se está haciendo uso del mismo.

805. La lista de redes preferidas (PNL) está disponible a través del menú "Ajustes - Wi-Fi" (ver apartado "5.14.4. Lista de redes preferidas (PNL)"). En el caso de redes no disponibles, aparecerán al final de la lista de redes, identificadas con el texto "Fuera de rango". En el caso de redes disponibles, aparecerán a lo largo de la lista de redes (según la intensidad de su señal), identificadas con el texto "Guardado" (si no es la red a la que está conectado el dispositivo móvil actualmente) o "Conexión establecida" (si se trata de la red a la que está conectado el dispositivo móvil actualmente).

806. La lista de redes preferidas sólo está disponible cuando el interfaz Wi-Fi está habilitado, no siendo posible acceder a ellas (para su borrado o edición) si éste está deshabilitado:



807. Debe tenerse en cuenta que no existe la opción de desconectarse de la red a la que el dispositivo móvil está conectado actualmente. La única opción disponible es deshabilitar el interfaz Wi-Fi o seleccionar otra red conocida disponible.

808. Las redes Wi-Fi pueden ser configuradas en dos modos: oculto o visible. Las redes ocultas son aquellas que no especifican el nombre de la red (SSID, *Service Set IDentifier*) en las tramas de anuncio de *broadcast* o *beacons*, redes también conocidas como *nonbroadcast*. Las redes visibles son las que sí incluyen el nombre de red en esas tramas.

809. Desde el punto de vista de seguridad, y con el objetivo de proteger a los clientes de la red Wi-Fi, se recomienda no hacer uso de redes Wi-Fi ocultas.

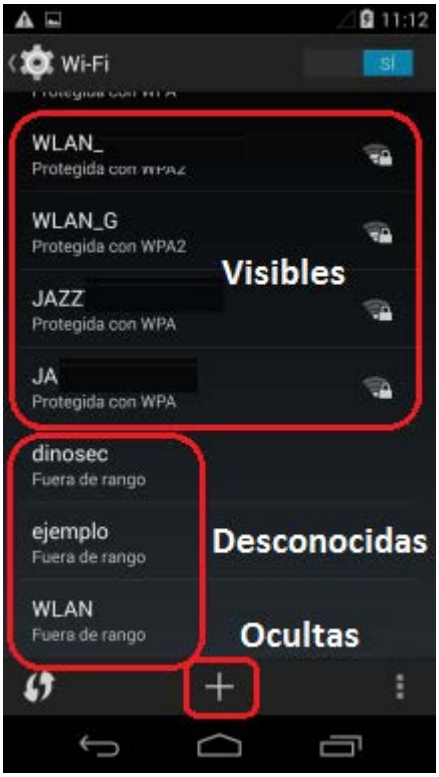
810. Aunque en primera instancia puede parecer que el uso de redes Wi-Fi ocultas es una opción más segura, en realidad no es así, ya que es sencillo para un potencial atacante descubrir su existencia e incluso el nombre de esas supuestas redes ocultas.

811. Sin embargo, el uso de una red oculta implica reducir el nivel de seguridad en los clientes Wi-Fi que se conectan a ella, como por ejemplo los dispositivos móviles basados en Android. Si una red está oculta, los clientes Wi-Fi se verán obligados a comprobar de forma explícita si está presente, generando tramas (de tipo *probe request*) dirigidas que desvelan necesariamente el nombre de la red, y lo que es más crítico, que les exponen frente a ataques de suplantación de dicha red por parte de un potencial atacante (especialmente cuando la red no emplea mecanismos de seguridad).

812. Desafortunadamente, Android no implementa ningún mecanismo explícito para definir si una red es oculta o no, por lo que en función de cómo se añada la red Wi-Fi al dispositivo móvil la primera vez, ésta será considerada como una red Wi-Fi oculta o visible.

813. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, seleccionándola de la lista de redes disponibles (situación que sólo se puede presentar si la red es visible), será añadida como red visible (escenario que aporta mayor seguridad a la configuración de Android).

814. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, manualmente mediante el botón "+" (signo más) disponible en la parte inferior central, bajo la lista de redes disponibles (situación necesaria a la hora de añadir redes ocultas), será añadida como red oculta (escenario vulnerable desde el punto de vista de Android):



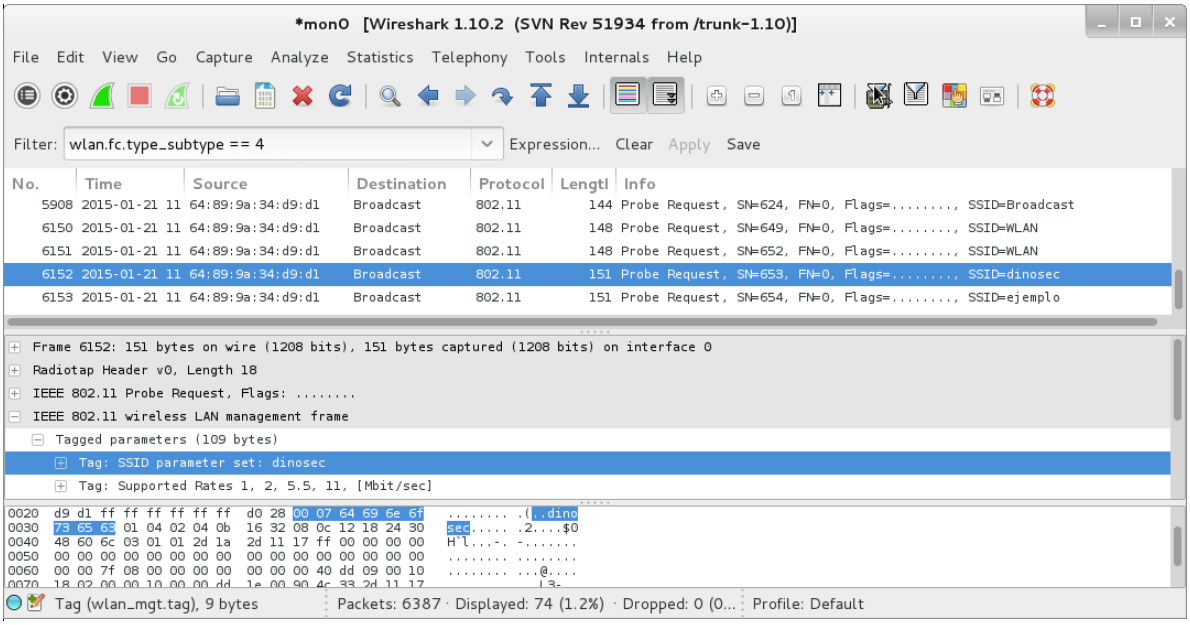
815. Este es el comportamiento más vulnerable (existente previamente pero corregido en algunos sistemas operativos y ordenadores portátiles y de sobremesa desde hace años), ya que obliga a Android a generar tráfico que desvela la lista de redes Wi-Fi configuradas en el dispositivo móvil (conocida como la PNL). Este comportamiento presenta un escenario similar al existente en equipos de escritorio basados en Windows XP sin la actualización de seguridad KB917021 aplicada, y conocida desde el año 2007 [Ref.- 50].

816. Adicionalmente, debe tenerse en cuenta que una vez una red Wi-Fi ha sido añadida al dispositivo móvil y está en la PNL, no se dispone de un mecanismo a través del interfaz gráfico de Android para determinar si es realmente considerada oculta o visible.

817. Resumiendo para todas aquellas redes configuradas o añadidas a través del botón "+" (signo más), Android generará tráfico que desvelará estas redes Wi-Fi disponibles en su lista de redes e intentará conectarse a ellas, escenario que puede ser empleado por un potencial atacante para disponer de conectividad con el dispositivo móvil y proceder a explotar vulnerabilidades en el mismo.

818. Por tanto, no se recomienda añadir ninguna red Wi-Fi manualmente al dispositivo móvil a través del botón "+", aunque es una práctica común desde el punto de vista de seguridad para disponer de mayor control sobre la configuración y ajustes de la red Wi-Fi a añadir.

819. En la imagen inferior, el dispositivo móvil Android intenta descubrir la presencia de las redes Wi-Fi disponibles en su PNL, "dinosec", "WLAN" y "ejemplo", una vez que el interfaz Wi-Fi ha sido activado, así como periódicamente, e incluso potencialmente aunque esté conectado a otra red Wi-Fi diferente en la actualidad:



820. Esta vulnerabilidad de revelación de información en función de cómo han sido añadidas las redes Wi-Fi a Android (manualmente o automáticamente desde la lista de redes Wi-Fi) ha sido confirmada por el Android Security Team (Google), aunque parece que no publicará una actualización para solucionarla [Ref.- 92].

Nota: la versión 2.2 de Android introdujo este cambio en el comportamiento de la pila de comunicaciones Wi-Fi, ya que en versiones previas (incluso versiones previas a 2.2 y la compilación FRF91 empleada para la elaboración de la presente guía) no era posible conectarse con redes Wi-Fi ocultas (tal como identifica el *bug* 1041 de Android [Ref.- 43]); en el pasado incluso aparecieron apps en Google Play para añadir esta funcionalidad.

En cualquier caso, siempre antes de poder establecer una conexión con una red Wi-Fi oculta es necesario añadirla al dispositivo móvil de forma manual, para que éste conozca su existencia, y pueda preguntar sobre su disponibilidad (empleando el comportamiento vulnerable descrito previamente).

821. Desafortunadamente, los dispositivos móviles Android no sólo desvelan el contenido de su PNL cuando disponen de redes Wi-Fi ocultas configuradas, sino también en numerosos otros escenarios [Ref.- 191].

822. En concreto, el dispositivo móvil empleado para la elaboración de la presente guía desvela su PNL continuamente, incluyendo tanto las redes Wi-Fi ocultas como visibles existentes en la misma.

5.14.6 PUNTO DE ACCESO O ZONA WI-FI

823. Android dispone de capacidades nativas para actuar como punto de acceso o zona Wi-Fi y router (o enrutador) hacia Internet, proporcionando acceso a múltiples dispositivos (u ordenadores, hasta un máximo de 10) vía Wi-Fi a su conexión de datos de telefonía móvil (2/3/4G) [Ref.- 91]. Para ello es necesario habilitar la conexión de datos móviles previamente (ver apartado "5.16. Comunicaciones móviles: voz y datos").

824. Para hacer uso de estas capacidades es necesario acceder al menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Anclaje a red y zona Wi-Fi":

825. A través de la opción "Zona Wi-Fi portátil" es posible habilitar el servicio de punto de acceso Wi-Fi (referido en ocasiones como *hotspot* o zona Wi-Fi), de forma que otros ordenadores y dispositivos puedan utilizar el dispositivo móvil como punto de acceso Wi-Fi para conectarse a Internet a través de su conexión de datos de telefonía móvil (2/3/4G).

826. Curiosamente, la zona Wi-Fi puede ser activada en Android incluso aunque el dispositivo móvil no disponga de conexión de datos a través de las redes de telefonía móvil, o incluso sin insertar una tarjeta SIM.

827. Debe tenerse en cuenta que, a diferencia del interfaz Wi-Fi (cliente) y Bluetooth, para poder llevar a cabo la configuración del punto de acceso Wi-Fi a través del interfaz de usuario del dispositivo móvil no es obligatorio activar esta funcionalidad, por lo que se recomienda modificar y completar su configuración antes de activar la funcionalidad, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:

828. Mediante la opción "Configurar zona Wi-Fi", es posible configurar los diferentes ajustes del punto de acceso, incluyendo el nombre de la red Wi-Fi (o SSID) y las características de seguridad:

829. Por defecto, el punto de acceso Wi-Fi hace uso de WPA2-PSK (Pre Shared Key, o WPA2-Personal), basado en el uso de una contraseña o clave precompartida, opción recomendada desde el punto de vista de seguridad. Android permite también la creación de puntos de

acceso Wi-Fi mediante WPA-PSK o abiertos ("Ninguna"), es decir, que no implementen ningún mecanismo de seguridad (opción desaconsejada).

830. Por defecto el dispositivo móvil selecciona una contraseña aleatoria de 12 caracteres de longitud, hexadecimales. Sin embargo, se recomienda hacer uso de una contraseña propia, de mayor longitud y recordable más fácilmente.

831. Cuando el dispositivo móvil actúa de punto de acceso Wi-Fi, las apps de Android no pueden utilizar la conexión Wi-Fi como dispositivo cliente. Si previamente a su activación la conexión Wi-Fi cliente estaba activa, ésta será deshabilitada automáticamente. Igualmente, tras desactivar el punto de acceso Wi-Fi, la conexión Wi-Fi cliente será habilitada de nuevo automáticamente.

832. Se recomienda no habilitar las capacidades de punto de acceso Wi-Fi en el dispositivo móvil salvo que se quiera hacer un uso limitado y controlado de esta funcionalidad. En caso de ser utilizada, la red Wi-Fi asociada debe ser protegida y configurada mediante WPA2-PSK con una contraseña o clave precompartida suficientemente larga (más de 20 caracteres) y difícilmente adivinable [Ref.- 49].

833. El mecanismo de cifrado para WPA2-PSK empleado por defecto por el punto de acceso Wi-Fi proporcionado por Android es AES-CCMP, opción recomendada desde el punto de vista de seguridad.

834. En caso de activar el punto de acceso Wi-Fi, se recomienda también modificar el nombre de la red Wi-Fi (o SSID) anunciada por el dispositivo móvil por defecto ("AndroidAP"), con el objetivo de no desvelar que se trata de un punto de acceso basado en Android:

835. La red Wi-Fi creada es de tipo punto de acceso (o infraestructura), se anuncia en el canal 6 (de 802.11b/g/n), y proporciona incluso capacidades de servidor DHCP para la asignación de direcciones IP a los dispositivos cliente y ordenadores que se conectan a ella.

836. Tras establecerse la conexión de red a través de la red Wi-Fi creada por Android, y tomando Windows 7 como sistema operativo del ordenador de referencia, el interfaz de red Wi-Fi funciona al estar configurado con una dirección IP dinámica (DHCP), asignándose por defecto una dirección IP de clase C (/24), como por ejemplo 192.168.43.17.

837. El dispositivo móvil (por ejemplo, con dirección IP 192.168.43.1) actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

Nota: el direccionamiento IP empleado por Android para el punto de acceso Wi-Fi (192.168.43.x) no puede ser modificado salvo en dispositivos móviles *rooted* [Ref.- 96].

838. La dirección MAC asociada al interfaz de red del punto de acceso Wi-Fi tiene asociado un OUI con valor "0**2**:1A:11" (por ejemplo), qué corresponde a una dirección MAC administrada localmente y, por tanto, no asignada a ningún vendedor públicamente.

839. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red empleado para el punto de acceso Wi-Fi del dispositivo móvil permite obtener las siguientes conclusiones:

- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por Nmap como "dnsmasq 2.51".
- Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).

840. Es posible interrumpir la disponibilidad del punto de acceso Wi-Fi deshabilitando la opción "Zona Wi-Fi portátil" habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red Wi-Fi.

5.14.7 WI-FI DIRECT ("P2P")

841. La tecnología Wi-Fi Direct, un estándar publicado por la Wi-Fi Alliance [Ref.- 53], permite el establecimiento de conexiones Wi-Fi directamente entre dispositivos, punto a punto ("P2P", Peer-to-Peer), sin hacer uso de una infraestructura, red o punto de acceso Wi-Fi.

842. Wi-Fi Direct (y sus servicios asociados) permite a un dispositivo móvil interactuar con otros dispositivos directamente, como por ejemplo mostrar su pantalla y cualquier contenido multimedia (o juegos) en un televisor, monitor o proyector[74], imprimir un documento en una impresora inalámbrica, compartir e intercambiar ficheros con otros dispositivos, como por ejemplo cámaras, o sincronizar datos con un ordenador.

843. Para hacer uso de Wi-Fi Direct no es necesario disponer de conexión a Internet, aunque esta tecnología también puede ser empleada para compartir el acceso a Internet de un dispositivo con otros dispositivos compatibles con Wi-Fi Direct.

844. Wi-Fi Direct permite tanto conexiones individuales entre dos dispositivos, como conexiones en grupo de varios dispositivos. Un dispositivo se encargará de proporcionar la red o el grupo Wi-Fi Direct, actuando como punto de acceso (denominado GO, Group Owner) y de gestionar dicha red y su conectividad (por ejemplo, proporcionando un servidor DHCP).

[74] Por ejemplo, las conexiones multimedia Miracast pueden ser llevadas a cabo sobre Wi-Fi Direct.

845. El establecimiento de las conexiones Wi-Fi Direct se puede llevar a cabo mediante la pulsación de un botón, acercando dos dispositivos con capacidades NFC, o mediante la introducción de un PIN, empleando el estándar Wi-Fi Protected Setup (WPS).

846. La especificación técnica asociada a Wi-Fi Direct, y denominada Wi-Fi Peer-to-Peer ("P2P") define mecanismos para que los dispositivos puedan anunciar y descubrir los servicios ofrecidos por otros dispositivos cercanos a través de Wi-Fi Direct.

847. Adicionalmente, a finales de 2014 se ratificó la estandarización de algunas mejoras de los servicios Wi-Fi Direct para llevar a cabo las tareas más comunes de forma sencilla, bajo el principio "descubrir, conectar y hacer" en un sólo paso, como por ejemplo[75]: (Wi-Fi Direct) "Send", para el envío de contenidos, "Print", para la impresión de documentos, "for DLNA", para el descubrimiento de dispositivos, y "Miracast", para la transmisión de contenidos multimedia.

848. La comunicación Wi-Fi Direct hace uso de WPA2 con AES para cifrar y autentificar los datos intercambiados.

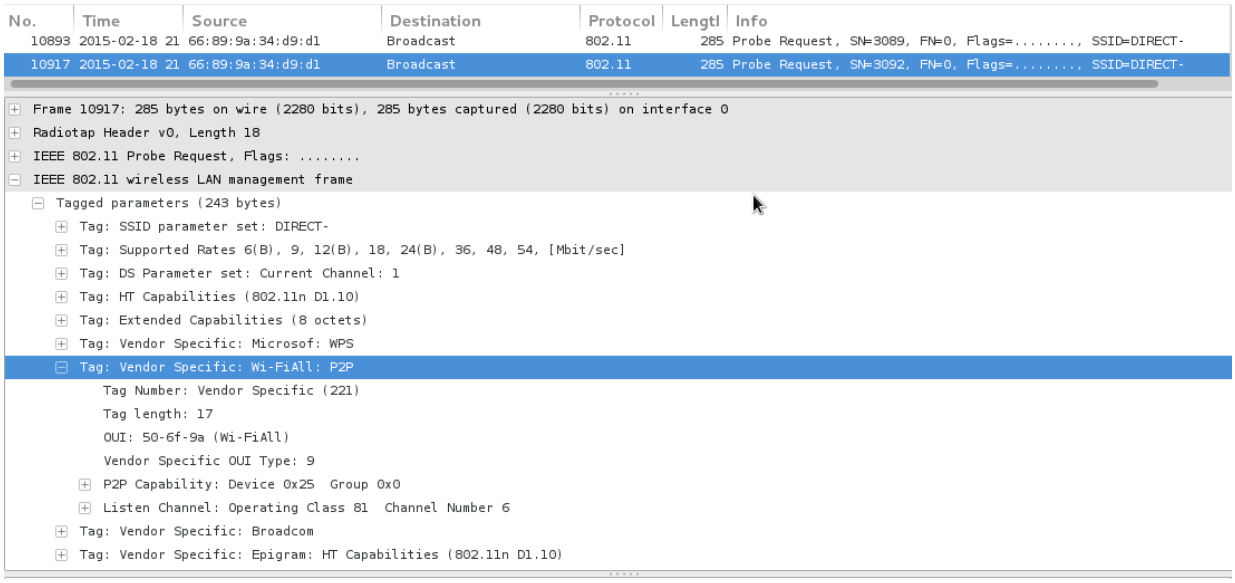
849. Las capacidades de Wi-Fi Direct, en concreto para iniciar una comunicación desde Android, están disponibles a través del menú "Ajustes - Wi-Fi - [...] - Wi-Fi Direct", siendo necesario que el interfaz Wi-Fi esté activo:

850. Tras acceder a dicho menú, el dispositivo móvil Android comienza a buscar a otros dispositivos con capacidades Wi-Fi Direct, tal como indica el botón inferior ("Buscando..."); ver imagen superior derecha.

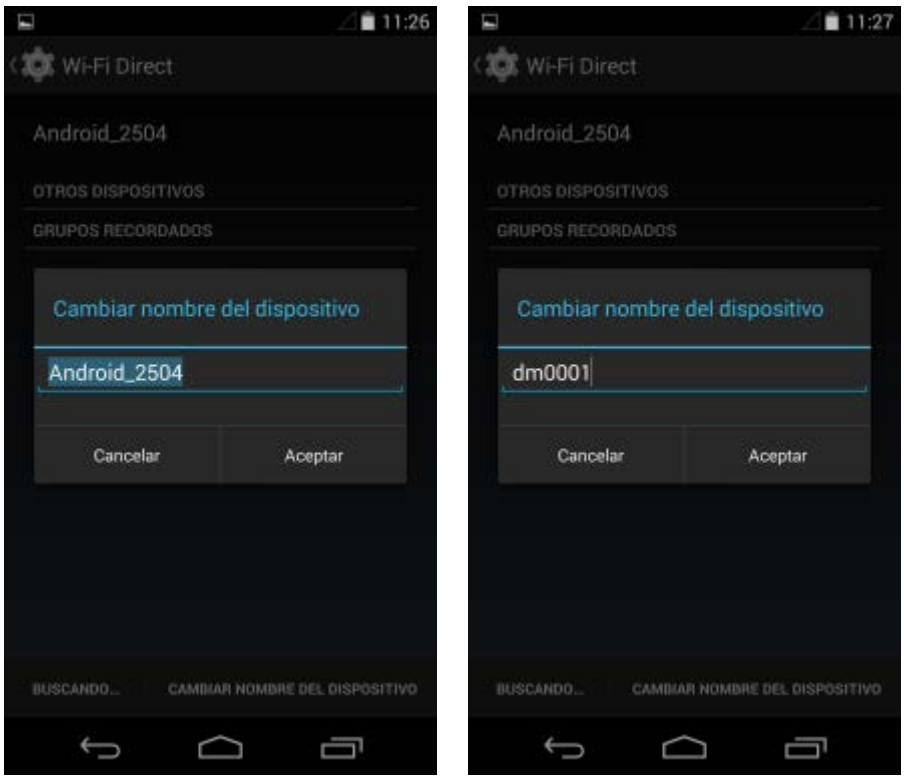
851. Para ello, envía tramas de tipo *probe request* con el nombre de red, o SSID, "DIRECT-" por defecto, y que desvelan el uso de Wi-Fi Direct. Adicionalmente, estas tramas 802.11 incluyen un campo asociado a Wi-Fi Direct (o P2P) con el valor "Wi-FiAll", y que

[75] http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-enhances-wi-fi-certified-wi-fi-direct

contiene detalles de sus capacidades P2P ("P2P Capabilities"), tanto a nivel de dispositivo como de grupo, y el canal en el que escucha:



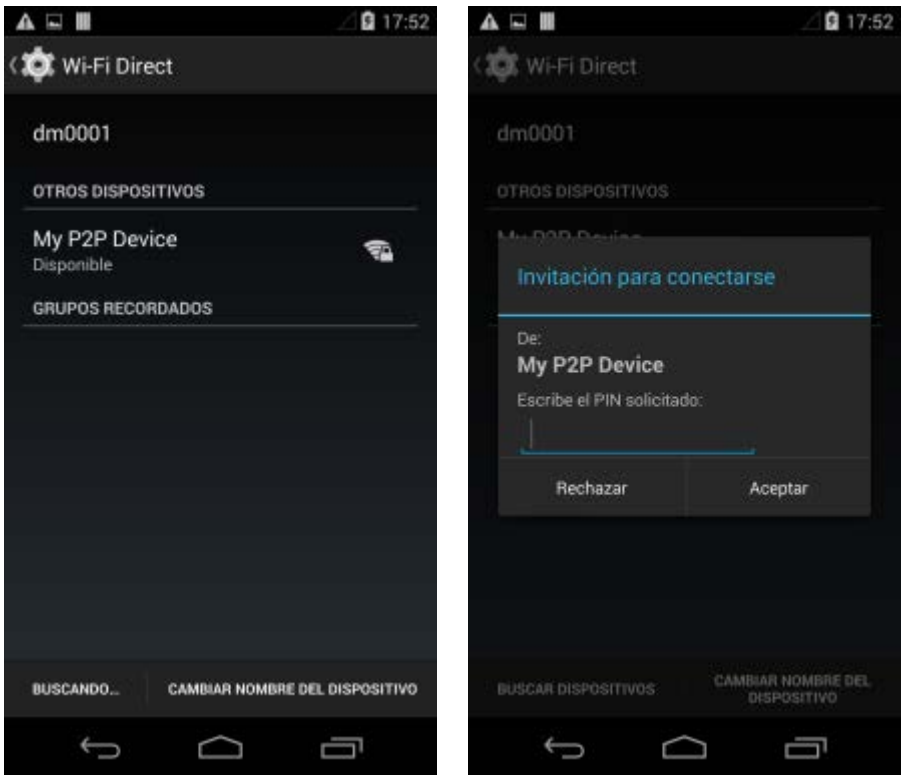
852. Por defecto, el nombre empleado por Android en Wi-Fi Direct es "Android_2504", donde "2504" corresponde con el comienzo del número asociado al nombre o *hostname* empleado por el dispositivo móvil, "android-25049d5b6e7d2d59" (ver apartado "5.9. Configuración por defecto del dispositivo móvil" [76]), por lo que se recomienda modificarlo a través del botón inferior "Cambiar Nombre del Dispositivo" (para Wi-Fi Direct) por un valor que no desvele ningún detalle del terminal, como por ejemplo "dm0001" ("dispositivo móvil 0001"):



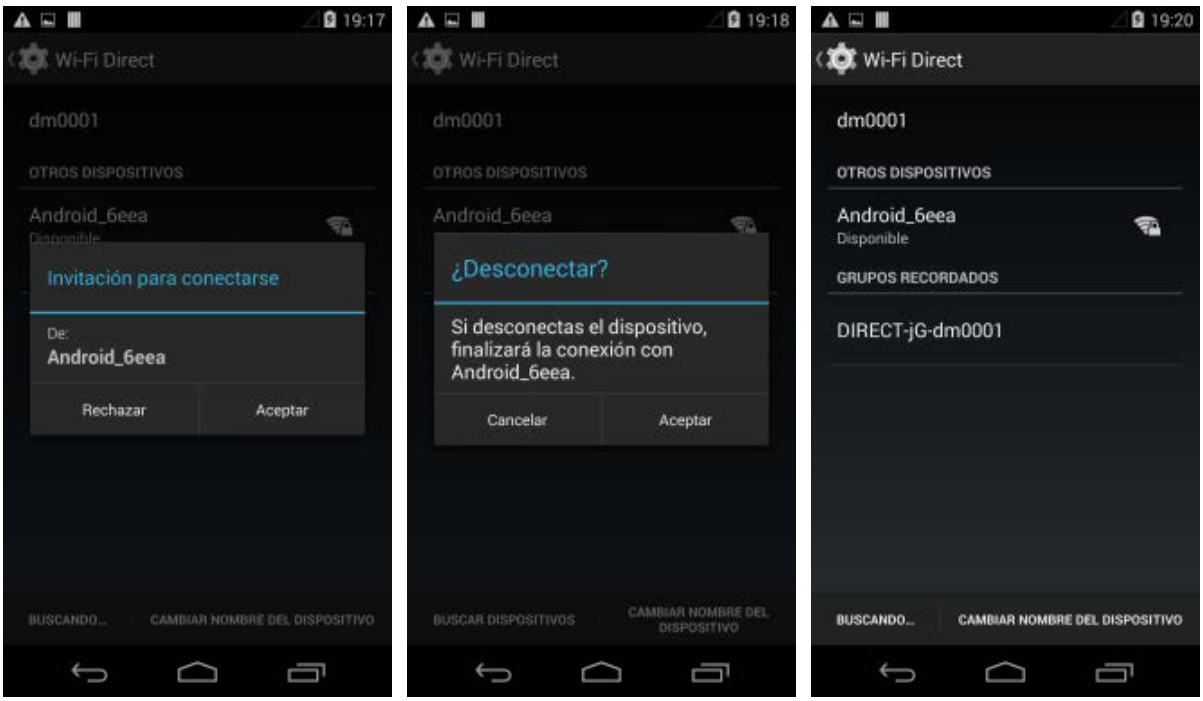
[76] El valor numérico del nombre cambia aleatoriamente tras restablecer los valores de fábrica.

853. Android emplea como dirección MAC para las conexiones Wi-Fi Direct una variante de la dirección MAC del interfaz Wi-Fi, convirtiéndola en una dirección administrada localmente. Por ejemplo, la dirección Wi-Fi que comienza por "64:89:9a" es convertida a "66:89:9a", respetando el resto de bytes de la dirección.

854. Una vez el dispositivo móvil descubre otros dispositivos con capacidades Wi-Fi Direct, puede iniciar una comunicación enviando una invitación para establecer la conexión:



855. Asimismo, el dispositivo móvil puede recibir una invitación de comunicación mediante Wi-Fi Direct proviniente de otros dispositivos:



856. En enero de 2015 fue publicada una vulnerabilidad de denegación de servicio (DoS) sobre Wi-Fi Direct que afecta a los dispositivos móviles Android con diferentes versiones 4.x, identificada por el CVE-2014-0997 [Ref.- 73]. En concreto, el dispositivo móvil empleado para la elaboración de la presente guía, con la última versión de Android KitKat disponible, Android 4.4.4, es vulnerable. La vulnerabilidad fue solucionada en Android 5.x (Lollipop), versiones 5.0.1 y posteriores.

857. Cuando el dispositivo móvil Android busca otros dispositivos con capacidades Wi-Fi Direct mediante las tramas de tipo *probe request* previamente descritas, si recibe una trama dirigida a su dirección MAC de tipo *Probe Response* malformada, el subsistema Dalvik no gestiona correctamente esta excepción, y en consecuencia, el dispositivo móvil se reiniciará parcialmente[77], no pudiendo hacer uso de Wi-Fi Direct hasta que cese el ataque. Este ataque es válido tanto si el dispositivo móvil está conectado a una red Wi-Fi conocida, como si no.

5.15 COMUNICACIONES MÓVILES: MENSAJES DE TEXTO (SMS)

858. Las capacidades de mensajería de texto (SMS, *Short Message Service*) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (*Global System for Mobile communications*, o 2G), UMTS (*Universal Mobile Telecommunications System*, o 3G) y LTE (*Long Term Evolution* o 4G).

859. El primer nivel de protección asociado al sistema de mensajería de texto pasa por la concienciación del usuario desde el punto de vista de seguridad, teniendo en cuenta que la implementación de este módulo en los dispositivos móviles actuales proporciona numerosas funcionalidades, y no únicamente la visualización de mensajes de texto.

860. Entre las funcionalidades avanzadas se encuentra la posibilidad de mostrar contenidos de texto, contenidos web (enlaces, HTML, JavaScript, etc.), gestionar datos binarios, como tonos de llamada, e intercambiar ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (*Enhanced Messaging Service*) y MMS (*Multimedia Message Service).*

861. Debido a las diferentes vulnerabilidades asociadas al módulo de mensajería de texto existentes en el pasado en múltiples dispositivos móviles actuales, incluyendo Android [Ref.- 1], se recomienda que el usuario actúe con prudencia ante la lectura de nuevos mensajes de texto, especialmente los recibidos de fuentes desconocidas.

862. Durante el año 2009 se publicaron diferentes vulnerabilidades de denegación de servicio (DoS) en el módulo SMS de dispositivos Android [Ref.- 1]. El proceso que gestiona los mensajes SMS en Android (SMSManager[78] o Provider) es una aplicación Java:

[77] No se lleva a cabo un reinicio completo del dispositivo móvil, sino sólo de algunos componentes críticos.
[78] http://developer.android.com/reference/android/telephony/SmsManager.html

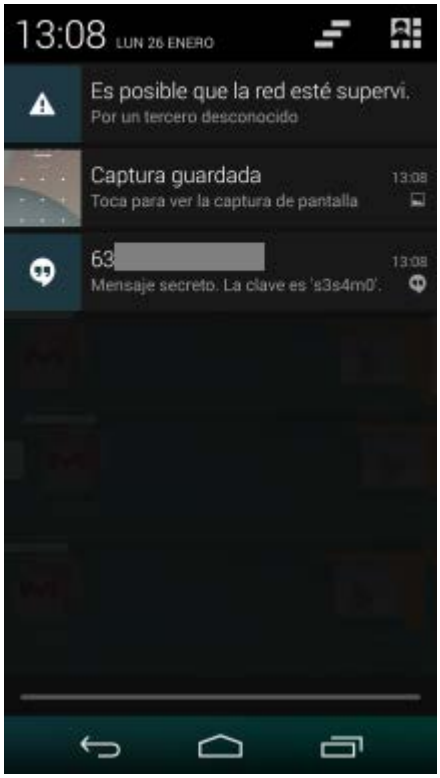
863. Se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos (o e-mails). A la hora de acceder y procesar los contenidos del buzón de entrada de mensajes de texto del dispositivo móvil, el usuario debería seguir las mejores prácticas de seguridad, como por ejemplo:

- No deberían abrirse mensajes de texto recibidos desde números desconocidos, ni ejecutar o permitir la instalación de contenidos adjuntos (configuraciones, binarios o multimedia) asociados a mensajes SMS/MMS no esperados.
- En su lugar, se debería proceder a borrar el mensaje directamente.
- En caso de acceder a los mensajes, debería desconfiarse de su contenido, y tener especial cuidado, por ejemplo, con la utilización de enlaces a sitios web externos.

864. Adicionalmente, es necesario tener en cuenta que los mensajes de texto pueden contener información sensible y confidencial. Por ejemplo, al gestionar el buzón de voz de un usuario, los operadores de telefonía móvil pueden enviar todos los detalles de acceso al buzón de voz, incluido el PIN, mediante un mensaje de texto. El acceso a dicho mensaje por parte de un potencial atacante permitiría disponer de control completo del buzón de voz del usuario.

865. Los nuevos mecanismos de autentificación de la banca online también emplean los mensajes de texto para el envío de contraseñas de un solo uso para la realización de operaciones bancarias críticas. El acceso a dicho mensaje por parte de un potencial atacante permitiría completar la operación, como por ejemplo, una transferencia bancaria.

866. La recepción de mensajes SMS por parte del dispositivo móvil cuando la pantalla de acceso está bloqueada, por defecto, únicamente muestra un icono en la barra superior de estado indicando que se ha recibido un mensaje SMS, pero no su contenido. Para acceder a su contenido es necesario desbloquear el dispositivo móvil y acceder al centro de notificaciones, donde se dispone de acceso a los contenidos confidenciales del SMS:

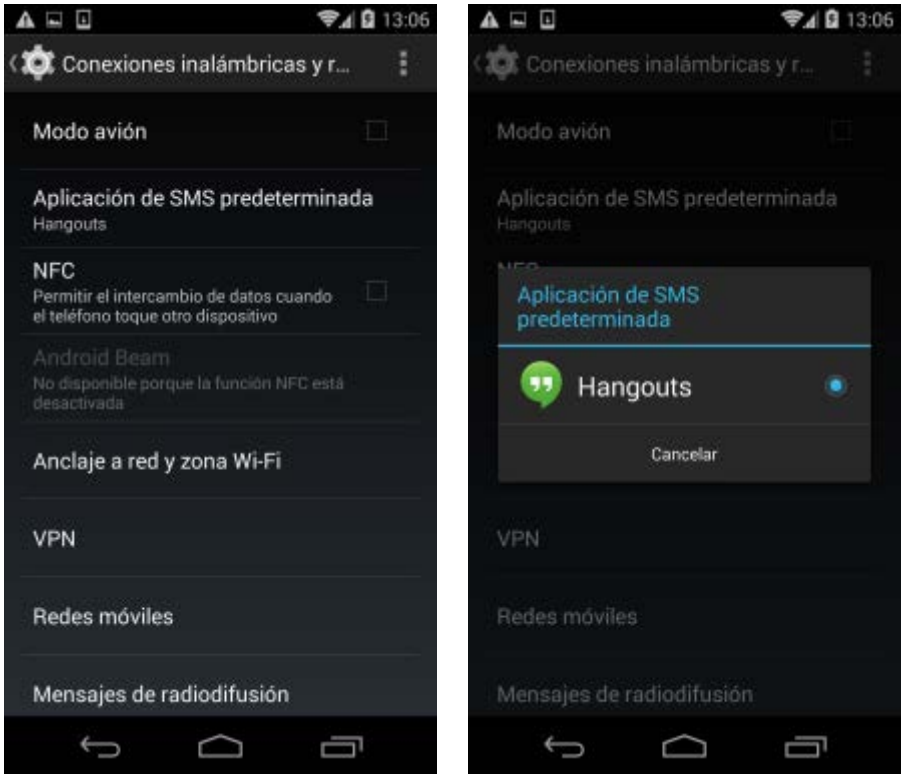


867. Por otro lado, el envío de mensajes de texto (SMS) a servicios *Premium* ha sido una técnica muy comúnmente utilizada por software malicioso (*malware*) móvil para obtener beneficios económicos. Especialmente, esta técnica de obtención de financiación de manera ilegal ha sido empleada al infectar dispositivo móviles basados en Android, debido a las facilidades existentes para el envío de SMS *Premium* en esta plataforma móvil y al coste asociado para el usuario por cada mensaje enviado (por ejemplo, un euro por SMS).

868. Por este motivo, Android 4.2 introdujo nuevos mecanismos de protección a la hora de enviar mensajes SMS *Premium*, por ejemplo por parte de una app, generándose un mensaje de notificación que debe ser aprobado por el usuario antes de proceder al envío del SMS al servicio *Premium*, con cargos adicionales [Ref.- 83].

869. Por otro lado, desde Android 4.4 (KitKat), la plataforma permite definir cuál es la app por defecto encargada de la gestión de mensajes SMS (*default SMS app*) [Ref.- 30], pudiendo haber únicamente una app gestionando la entrada de nuevos SMS (o MMS) al dispositivo móvil, y especialmente, disponiendo de capacidades de escritura en el proveedor de telefonía de Android.

870. La app por defecto encargada de la gestión de mensajes SMS se define a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Aplicación de SMS predeterminada" (por defecto asociada a la app "Hangouts"):



Nota: existen soluciones propietarias de cifrado de mensajes de texto (que reemplazan o complementan a los SMS) y de mensajería en general (chat), como TextSecure (de código abierto), proporcionadas por terceras compañías a través de Google Play, que cifran los mensajes de texto tanto durante su almacenamiento en el dispositivo móvil como durante su trasmisión a otros usuarios de la app TextSecure [Ref.- 33]. TextSecure hace uso del protocolo OTR (*Off The Record*), con mejoras[79], para cifrar los mensajes de texto. TextSecure puede ser empleado para el envío de mensajes cifrados entre terminales Android, o también con terminales basados en iOS mediante la app Signal[80], empleando las comunicaciones de datos (Wi-Fi o 2/3/4G) de los dispositivos móviles, o la infraestructura SMS de los operadores. El uso de la infraestructura de SMS asociada a los proveedores u operadores de telecomunicaciones para el envío de mensajes de texto puede revelar información en los metadatos de dichas conversaciones.

Actualmente, se dispone de otras soluciones similares, como por ejemplo Wickr [Ref.- 32], que hacen uso de mecanismos como PFS, *Perfect Forward Secrecy* (al igual que TextSecure).

5.16 COMUNICACIONES MÓVILES: VOZ Y DATOS

5.16.1 DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS MÓVILES

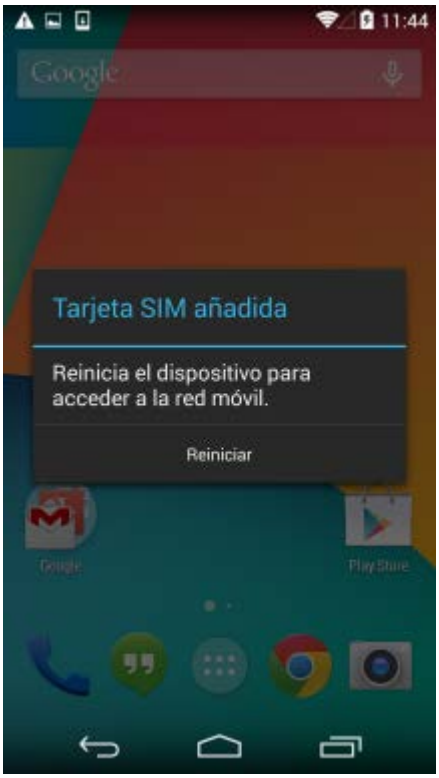
871. La principal recomendación de seguridad asociada a las comunicaciones de voz (y SMS) a través de las redes de telefonía móvil en dispositivos móviles es no activar las capacidades de telefonía del terminal salvo que se haga uso de éstas (situación muy habitual, al ser ésta una de las funcionalidades principales de los dispositivos móviles, especialmente en *smartphones* frente a tabletas, o *tablets*).

[79] https://whispersystems.org/blog/simplifying-otr-deniability/
[80] https://github.com/WhisperSystems/Signal-iOS

Nota: durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), el interfaz de telefonía móvil para comunicaciones de voz está habilitado, solicitando en primer lugar el PIN de la tarjeta SIM, si ésta está insertada.

Se recomienda desactivar el interfaz de telefonía móvil tan pronto finalice el proceso de configuración inicial, para proceder a la aplicación de las medidas de seguridad seleccionadas.

872. En Android 4.x, y en concreto para el dispositivo móvil analizado, cada vez que se inserta una nueva tarjeta SIM se notifica al usuario que es necesario reiniciar el dispositivo para poder hacer uso de las capacidades de telefonía móvil (acceso a la red móvil). Al extraer la tarjeta SIM también se muestra un mensaje similar:



873. Android únicamente permite a través del interfaz de usuario estándar deshabilitar de forma individualizada las capacidades de telefonía móvil (voz y SMS) a través de la opción "Modo avión" del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más...".

874. Al activar el modo avión en Android, tanto la conectividad a redes Wi-Fi como la conectividad de Bluetooth puede ser habilitada posteriormente y de forma independiente, mientras la conectividad de telefonía móvil sigue deshabilitada. No así la conectividad móvil 2/3/4G, directamente ligada al modo avión:

875. Adicionalmente, es posible obtener y configurar información avanzada a través del menú de prueba (o *testing*), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*). Esta funcionalidad permite independizar la desconexión de los diferentes interfaces de comunicaciones inalámbricos, es decir, Bluetooth, Wi-Fi y telefonía móvil 2/3/4G.

876. Sin activar el modo avión, independientemente del estado de activación de los interfaces Bluetooth y Wi-Fi, mediante la selección de la opción "Información sobre el teléfono" es posible desconectar únicamente el interfaz de telefonía móvil 2/3/4G::

877. Para ello es necesario seleccionar el botón "Desactivar señal móvil" en la parte inferior, y como resultado se desactivará únicamente y por completo (voz y datos) el interfaz de radio

de telefonía móvil, pudiendo permanecer los interfaces de Bluetooth y Wi-Fi activos, tal y como denotan los iconos de la barra superior de estado.

878. Este cambio de configuración no prevalece tras reiniciar el dispositivo móvil, dónde de nuevo el interfaz de radio de telefonía móvil será activado automáticamente tras introducir el PIN de la tarjeta SIM:

879. Por otro lado, la principal recomendación de seguridad asociada a las comunicaciones de datos a través de las infraestructuras de telefonía móvil en dispositivos móviles es no activar las capacidades de transmisión y recepción de datos salvo en el caso en el que se esté haciendo uso de éstas, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver, la pila de comunicaciones móviles y cualquiera de los servicios y apps disponibles a través de esa red y la conexión a Internet.

880. Las conexiones de datos a través de la red de telefonía móvil (2/3/4G), GPRS, UMTS o LTE, pueden ser deshabilitadas a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Uso de datos - Datos móviles" y en concreto el botón "[SI | NO]".

881. También pueden ser habilitadas a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles - Habilitar datos":

882. La opción "Itinerancia de datos" (o *roaming*), disponible a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles", permite configurar si se desea hacer uso de las capacidades de datos de telefonía móvil del dispositivo cuando se viaja al extranjero y el terminal se encuentra en una red de otro operador al asociado por defecto a su tarjeta SIM:

Nota: además de la seguridad, una de las preocupaciones de los usuarios de dispositivos móviles sin tarifa plana de conexión de datos son los cargos asociados al uso de las comunicaciones de datos a través de las redes de telefonía móvil (2/3/4G), especialmente cuando el contrato tiene gastos asociados por la cantidad de datos transmitidos y/o por tiempo o número de conexiones establecidas, o se viaja internacionalmente (itinerancia o *roaming*). Múltiples apps en Android pueden iniciar este tipo de conexiones de datos en diferentes momentos del día.

883. Por defecto en Android (configuración de fábrica) el interfaz de datos de telefonía móvil está habilitado (con los APNs que han sido definidos por la tarjeta SIM empleada).

884. Android mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil, es decir, si el interfaz de telefonía de datos estaba activo al apagar el terminal, al encender el dispositivo móvil e introducir el PIN de la tarjeta SIM, seguirá activo.

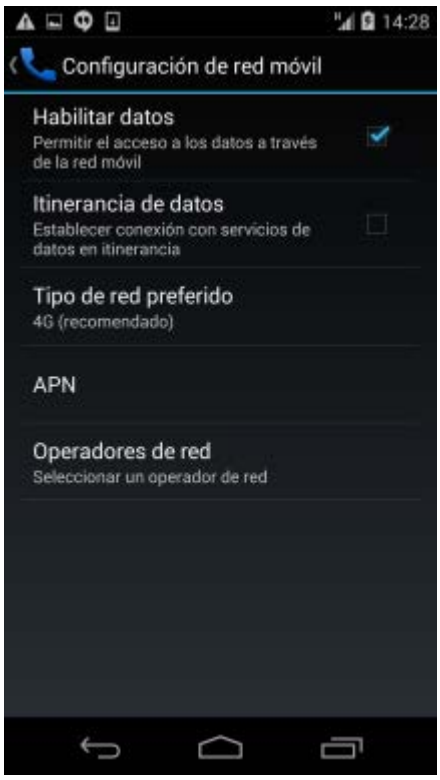
885. Igualmente, al salir del modo avión el estado del interfaz de datos de telefonía móvil será restaurado, y se activará en el caso de haber estado activo previamente (antes de activar el modo avión).

886. Tras desactivar la conexión de datos, si alguna app requiere disponer de conectividad (por ejemplo, acceso a la web desde el navegador web existente por defecto) la conexión de telefonía de datos no será activada automáticamente.

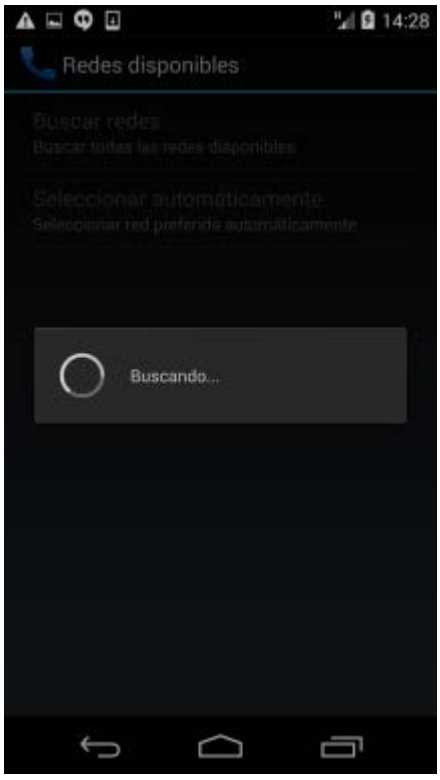
5.16.2 CONFIGURACIÓN Y SELECCIÓN DE LA RED (VOZ) DE TELEFONÍA MÓVIL

887. Android permite al usuario utilizar la red de telefonía móvil configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual el operador de telecomunicaciones móviles (voz y SMS).

888. Desde el menú de configuración del teléfono ("Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles") y a través de la opción "Operadores de red", es posible acceder a las opciones para seleccionar el operador de red, ya sea de forma automática como manual:



889. Android llevará a cabo una búsqueda automática de las redes disponibles en la ubicación actual del dispositivo móvil, y mostrará al usuario la lista de operadores de telecomunicaciones identificados (no mostrados en la imagen inferior derecha):



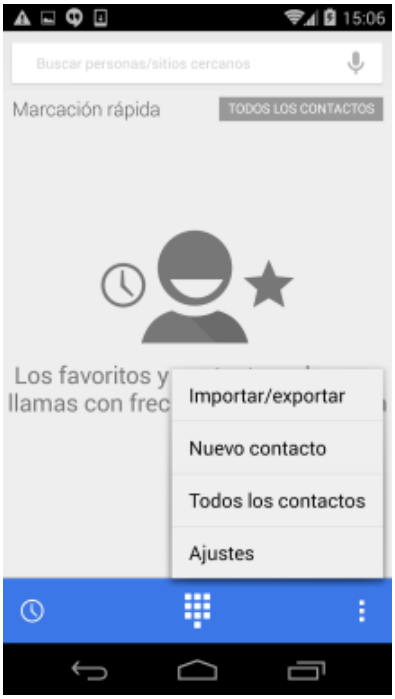
890. La selección de red permite definir si la red de telefonía será seleccionada de forma automática (opción por defecto) por el dispositivo móvil en función de la tarjeta SIM y de la intensidad de la señal, o sí el usuario puede definir de forma manual la red a la que desea conectarse de la lista de redes disponibles.

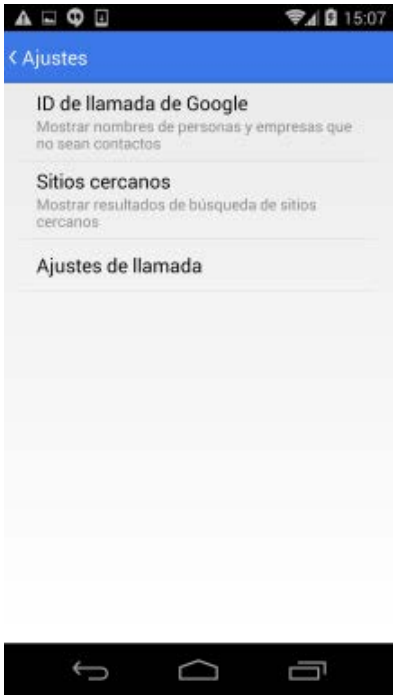
891. Adicionalmente, Android dispone en sus versiones más recientes de otras capacidades y ajustes de configuración asociados a la app del teléfono[81] que pueden tener implicaciones desde el punto de vista de seguridad.

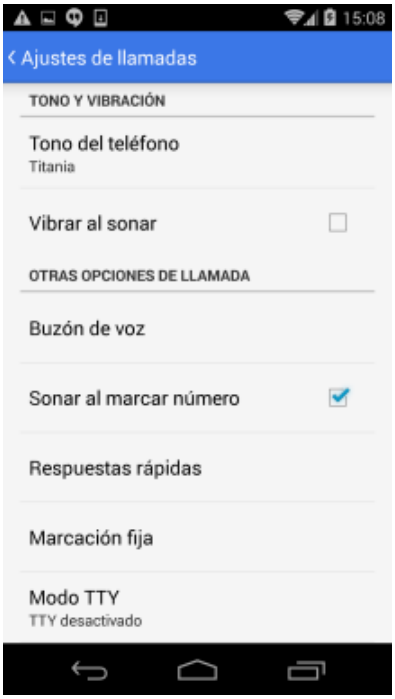
892. Con el objetivo de proteger la privacidad del usuario, el módulo de telefonía de Android, en concreto la app del teléfono, permite al usuario definir en qué tipo de llamadas se enviará la información de identificación como autor de la llamada: "Valor predeterminado de red" (opción por defecto), "Ocultar número" (siempre se ocultará) o "Mostrar número" (siempre se mostrará para todas las llamadas realizadas).

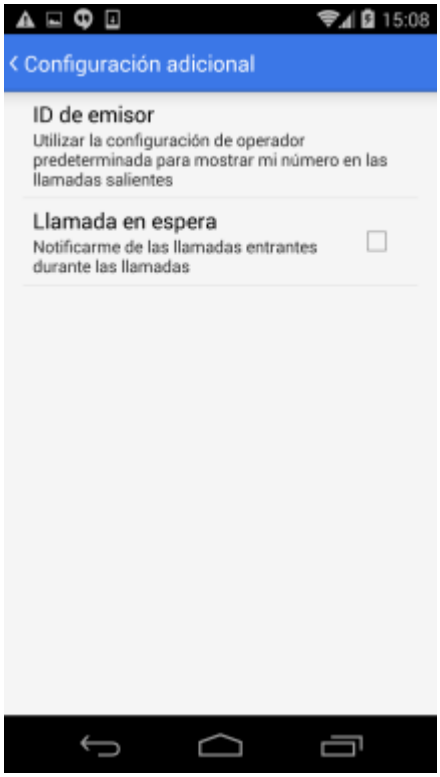
893. Desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte inferior derecha, a través del menú "Ajustes - Ajustes de llamada - Configuración adicional", mediante la opción "ID de emisor", es posible configurar la opción deseada:

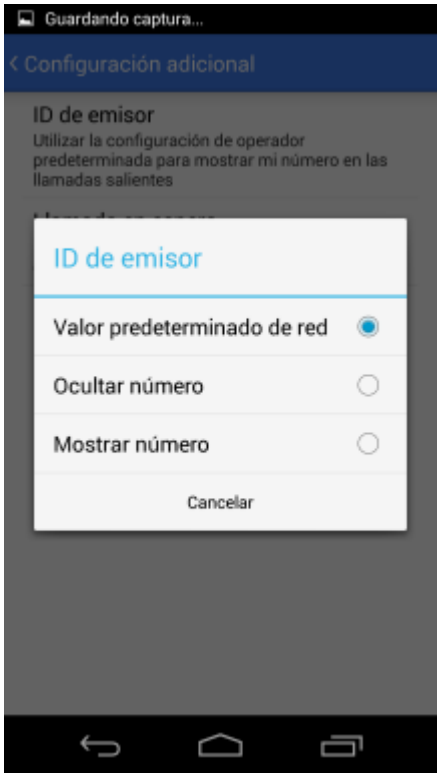
[81] https://support.google.com/nexus/answer/2895524









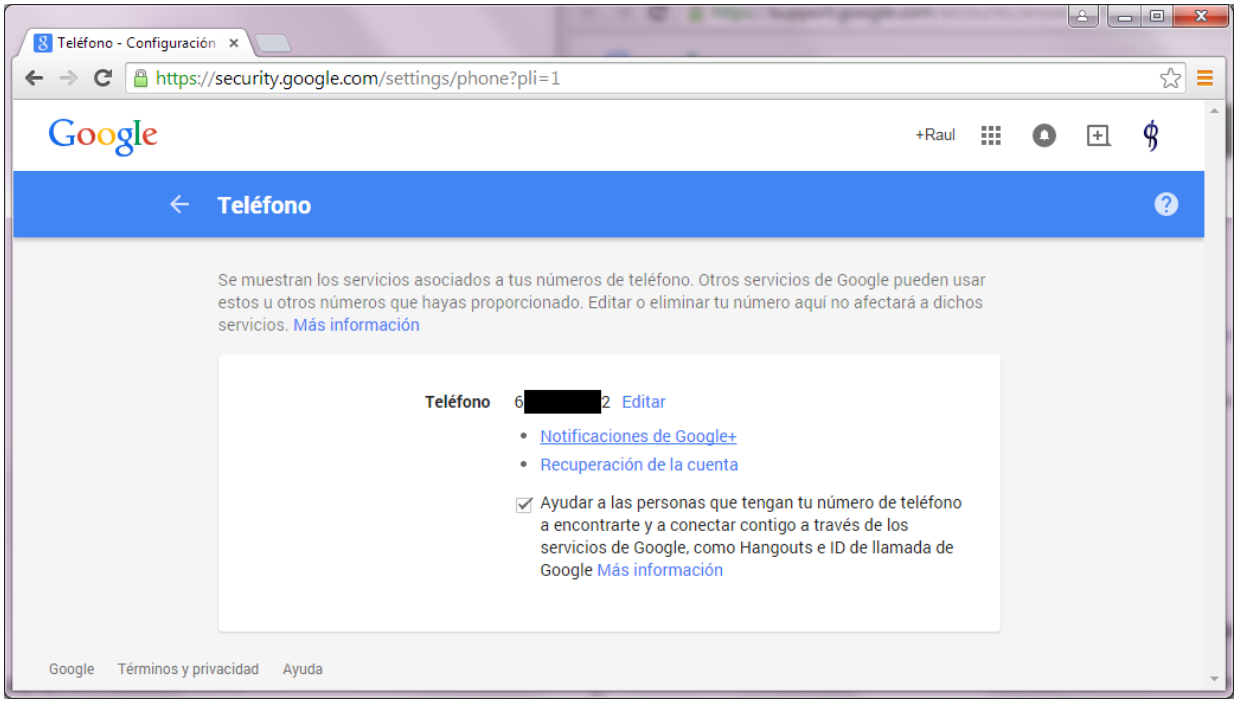


894. Desde la versión Android 4.4 (KitKat), Google ha implementado la identificación de llamadas inteligente, también denominada identificación de llamada de Google [Ref.- 145]. Cuando se recibe (o se realiza) una llamada de alguien que no está en la agenda o lista de contactos, el teléfono buscará coincidencias para las personas en base a la información disponible en su cuenta de usuario de Google (desde el año 2014[82]) y para las empresas que tengan una ficha local en Google Places (o Google Maps).

[82] https://plus.google.com/photos/+android/albums/5942570061497141729

895. En el caso de compañías y organizaciones que hagan uso de Google Apps, el teléfono buscará información del empleado que realiza la llamada en el directorio existente en Google Apps para la organización (si se están compartiendo los números de teléfono).

896. La visibilidad del número de teléfono propio para otras personas puede ser modificado a través de los ajustes de la cuenta de usuario de Google, en concreto, desde el siguiente enlace "https://www.google.com/settings/phone"[83] y la opción disponible en la parte inferior:

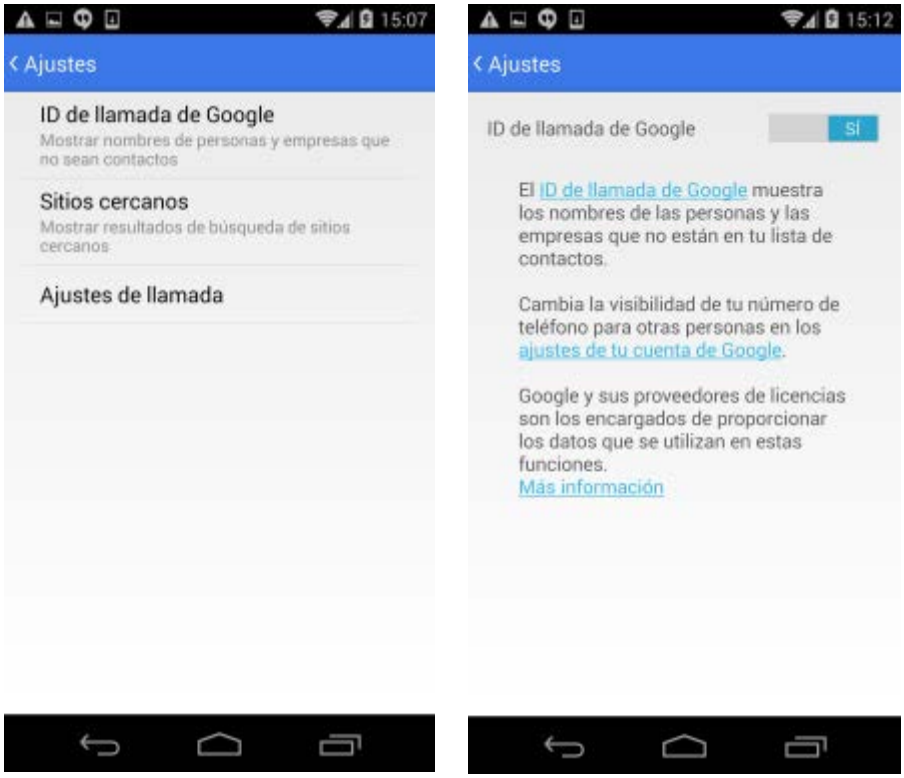


897. La modificación del número de teléfono asociado a la cuenta de usuario de Google afecta a los servicios de Google listados en la página web anterior. Debe tenerse en cuenta que existen numerosos servicios que pueden hacer uso del número de teléfono del usuario [84].

898. La visibilidad del número de teléfono en la cuenta de usuario de Google está habilitada por defecto, por lo que se recomienda deshabilitarla si no se desea compartir el número de teléfono propio con otros usuarios y que otras personas puedan hacer uso del mismo. Si está habilitada, otros usuarios podrían iniciar una conversación contigo (por ejemplo, mediante Hangout) empleando el número de teléfono, o ver tu nombre y foto de perfil cuando tú les llamas o al llamarte ellos[85], como parte de la funcionalidad del identificador de llamada de Google.

899. La configuración del uso de esta funcionalidad está disponible en Android desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte inferior derecha, a través del menú "Ajustes - ID de llamada de Google" (por defecto está habilitado):

[83] https://security.google.com/settings/phone
[84] https://support.google.com/accounts/answer/3463280?p=modifynumber
[85] https://support.google.com/accounts/answer/3113316

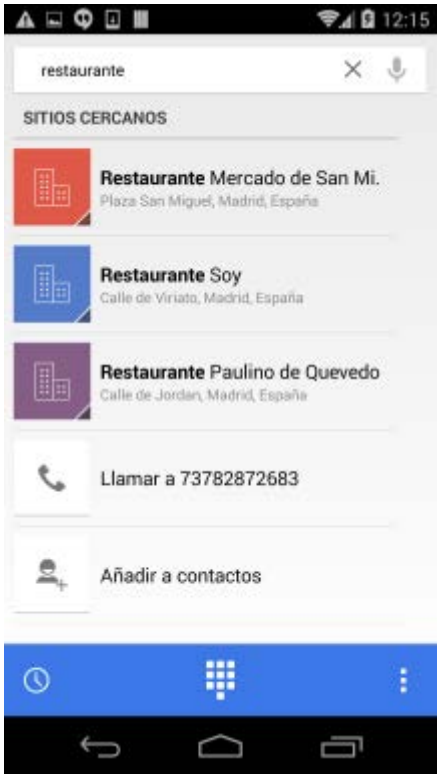


900. Los ID de llamada de Google no se añaden automáticamente a la lista de contactos. Desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

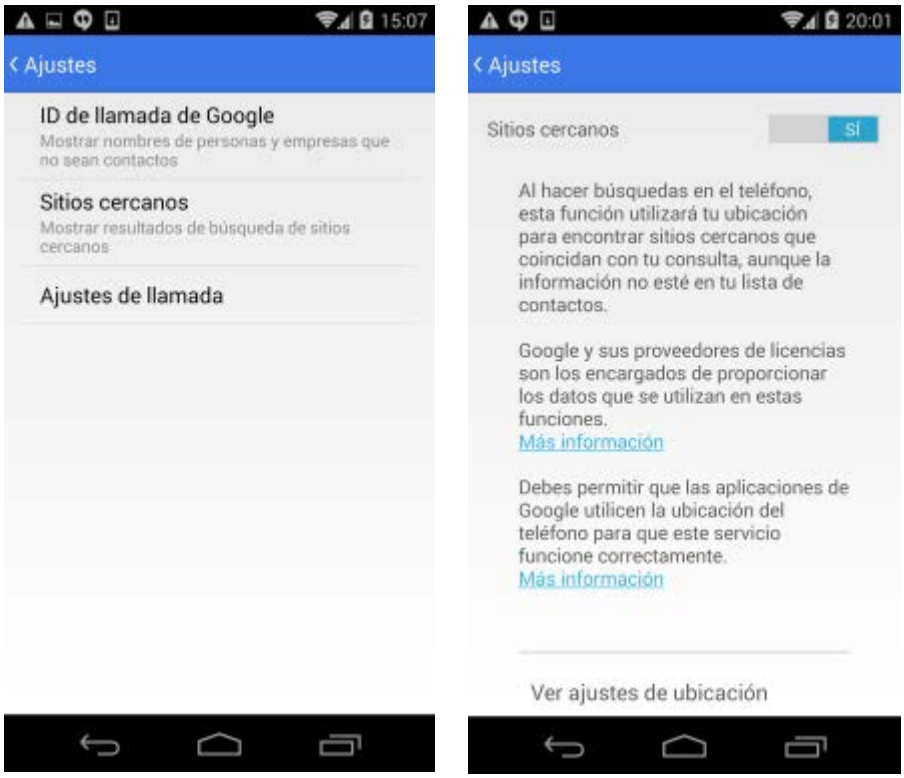
901. Es decir, por un lado desde la configuración del número de teléfono de la cuenta de usuario de Google es posible configurar si otros usuarios pueden localizarnos en base a nuestro número de teléfono, y por otro lado, desde los ajustes de la app teléfono en Android es posible configurar si deseamos localizar a otros usuarios (que lo permitan) a través de la funcionalidad del identificador de llamada de Google.

902. También en Android 4.4 se dispone de capacidades en el teléfono para utilizar la ubicación del dispositivo móvil para encontrar sitios cercanos que coincidan con las búsquedas realizadas en el teléfono, aunque la información proporcionada no esté disponible en la agenda o lista de contactos, actuando de guía telefónica.

903. Cuando se realiza una búsqueda en la agenda o lista de contactos desde la app teléfono, el teléfono buscará información relacionada de sitios cercanos y la mostrará en la parte superior:



904. La configuración de esta funcionalidad está disponible desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte inferior derecha, a través del menú "Ajustes - Sitios cercanos" (por defecto está habilitado):



905. Los teléfonos sugeridos de sitios cercanos no se añaden automáticamente a la lista de contactos, aunque sí se pueden guardar posteriormente de forma manual, mediante la opción "Añadir a contactos". De nuevo, desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

Nota: Android 4.4 (KitKat) permite la realización de llamadas por Internet (VoIP, *Voice over IP*) mediante el protocolo SIP (*Session Initiation Protocol*) de señalización si el proveedor de telefonía ofrece dichas capacidades y el dispositivo móvil está conectado a una red Wi-Fi[86].

Existen soluciones propietarias de cifrado extremo a extremo de las comunicaciones y llamadas de voz, como RedPhone (de código abierto), proporcionadas por terceras compañías a través de Google Play [Ref.- 29]. RedPhone hace uso del protocolo ZRTP para negociar las claves de cifrado empleadas en el protocolo SRTP, utilizado para cifrar las comunicaciones de Voz sobre IP (VoIP) entre dos terminales Android (o también con terminales basados en iOS mediante la app Signal[87]), haciendo uso de redes Wi-Fi o de la infraestructura de datos de los operadores de telefonía móvil, y empleando comunicaciones de datos cifradas mediante TLS con los servidores de RedPhone (para el protocolo de señalización) y mensajes SMS cifrados para el establecimiento de las llamadas.

5.16.3 CONFIGURACIÓN DE LA RED DE DATOS MÓVILES

906. Android permite al usuario, al igual que para la red de telefonía móvil (SMS y voz), utilizar la red de datos configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual tanto el operador de telecomunicaciones móviles como el APN (*Access Point Name*) para las conexiones de datos.

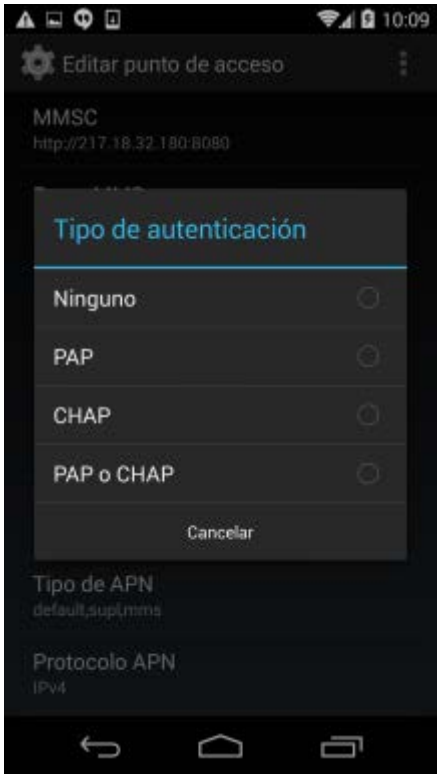
907. En dispositivos móviles Android como el empleado para la elaboración de la presente guía, al introducir la tarjeta SIM en el dispositivo móvil se lleva a cabo automáticamente el proceso de configuración de las opciones de conectividad de datos asociadas a las redes de telefonía móvil, incluyendo los APNs y su configuración: nombre, APN, proxy y puerto, credenciales (usuario y contraseña), servidor, dispositivos de mensajes multimedia (MMS: MMSC, proxy y puerto MMS), MCC, MNC, tipo de autentificación y tipo de APN.

908. En función de la tarjeta SIM empleada y de la configuración de datos que ésta tenga asociada, se mostrarán automáticamente los ajustes de conexión disponibles en la lista de APNs, o ningún APN si no dispone de los datos correspondientes (en cuyo caso habrá que añadirlo manualmente).

909. Desde el menú de configuración del teléfono, desde "Ajustes [Conexiones Inalámbricas y Redes] - Mas... - Redes móviles", y a través de la opción "APN", es posible acceder a las opciones para seleccionar el APN empleado para las conexiones de datos. Mediante la selección del APN de la lista es posible editar la configuración de los APNs existentes, y a través de los botones de la parte superior derecha es posible añadir nuevos APNs o restablecer la configuración inicial:

[86] https://support.google.com/nexus/answer/2811843
[87] https://github.com/WhisperSystems/Signal-iOS

910. Al definir un nuevo APN deben emplearse los valores proporcionados por el operador de telecomunicaciones. Desde el punto de vista de seguridad, y si el operador admite diferentes protocolos de autentificación, se recomienda seleccionar autentificación mediante CHAP, dentro de las cuatro alternativas disponibles en la opción "Tipo de autenticación" (Ninguno, PAP, CHAP, y "PAP o CHAP"). Por defecto en tipo de autentificación no está definido en el perfil del APN:



911. En el escenario de autoconfiguración existente por defecto, desde el punto de vista de seguridad, cada vez que se cambia la tarjeta SIM se recomienda acceder a la configuración de datos de telefonía móvil y, en concreto, a la lista de APNs para adecuar la configuración a la deseada por el usuario.

5.16.4 SELECCIÓN DE LA RED DE DATOS MÓVILES

912. Las redes de telefonía 2G (o GSM) presentan diferentes vulnerabilidades en la actualidad, como por ejemplo la posibilidad de suplantación de la red por parte de un potencial atacante debido a debilidades en los mecanismos de autentificación, o la posibilidad de capturar y descifrar el tráfico de voz GSM debido a debilidades en los algoritmos de cifrado, A5/1 [Ref.- 1].

913. Con el objetivo de mitigar las vulnerabilidades existentes actualmente en las redes de telefonía móvil 2G (o GSM), se recomienda forzar al dispositivo móvil a conectarse únicamente, tanto para comunicaciones de voz como de datos, a las redes de telefonía 3G (UMTS) o 4G (LTE).

914. Android no permite restringir las comunicaciones de telefonía móvil sólo a redes 3G o 4G a través del interfaz de usuario estándar (ver opciones mediante el menú de prueba o *testing* posteriormente).

915. A través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles", y en concreto de la opción "Tipo de red preferido", es posible indicar que sólo se haga uso de redes 2G (GSM - GPRS o EDGE), una opción indicada para disminuir el consumo de batería del terminal, pero desaconsejada desde el punto de vista de seguridad:

916. La opción por defecto es "4G (recomendado)". Se recomienda no modificar esta opción, especialmente al valor "2G", pese a que el dispositivo móvil hará uso automáticamente de redes 2G en zonas dónde no se disponga de suficiente cobertura por parte de las redes 3G o 4G.

917. El principal inconveniente de esta configuración (no modificable) es que si el usuario se encuentra en una zona dónde no se dispone de cobertura 3G (o superior, 3.5G o 4G), se podrá hacer uso del dispositivo móvil a través de 2G, premiando la disponibilidad del servicio de telefonía (voz y datos) por encima de la seguridad.

918. Android proporciona información en la barra superior de estado a través de un conjunto de iconos específico sobre las tecnologías de telefonía móvil de datos para las que se dispone de cobertura, que representan la disponibilidad y el estado de la conexión para una red 4G (LTE), 3G o 3.5G (WCDMA/UMTS o HSPA), 2.75G (EDGE) y 2G (GPRS).

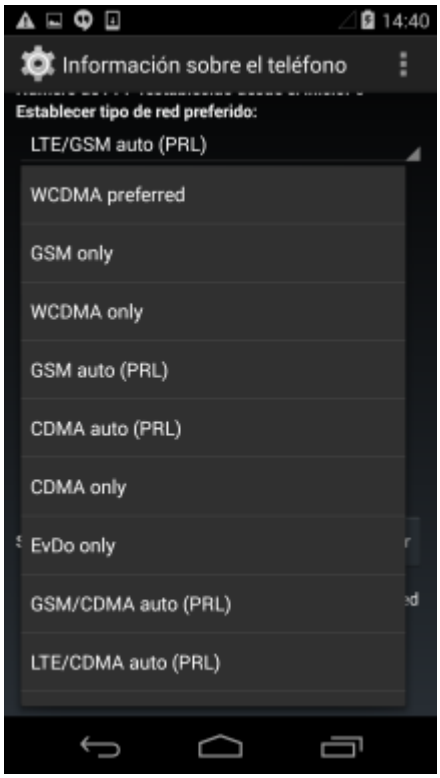
919. La cobertura y conectividad existentes están identificadas por un icono con forma de triángulo (barras en progresión ascendente), que indica la cobertura existente en función del número de barras activas, o que no se dispone de cobertura si el icono con forma de triángulo está vacío (no dispone de ninguna barra).

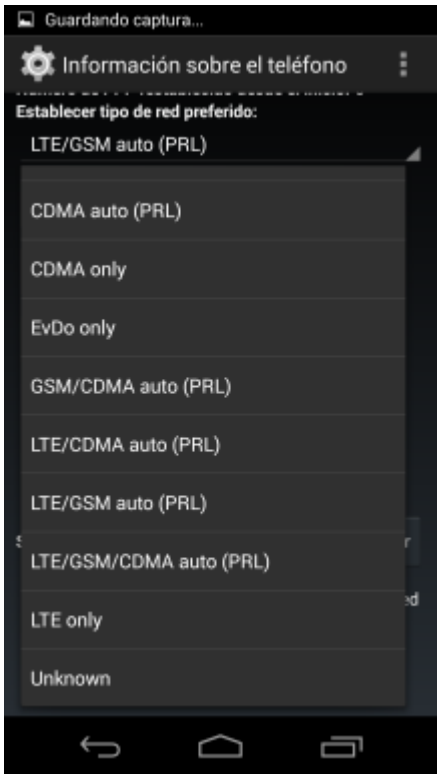
920. La configuración por defecto del dispositivo móvil premia la conectividad, permitiendo el uso de redes de telefonía móvil 2G, 3G o 4G de forma automática en función de su cobertura y disponibilidad.

921. Adicionalmente, es posible obtener y configurar información avanzada a través del menú de prueba (o *testing*), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*).

922. Mediante la selección de la opción "Información sobre el teléfono" se dispone de numerosos detalles de la red de telefonía móvil, siendo posible configurar el tipo de red preferida en la parte inferior de dicha pantalla, mediante la opción "Establecer tipo de red preferido":

923. De las diferentes opciones disponibles, desde el punto de vista de seguridad se recomienda seleccionar la opción "LTE only" o "WCDMA only" para forzar al dispositivo móvil a conectarse únicamente a redes 4G o 3G. Por defecto la opción seleccionada es "LTE/GSM auto (PRL)", donde el término PRL hace referencia a la "Preferred Roaming List" definida por los operadores de telefonía móvil:





924. Este cambio de configuración prevalece incluso tras reiniciar el dispositivo móvil y fuerza a que el dispositivo móvil sólo hago uso de redes 4G o 3G, más seguras que las redes 2G.

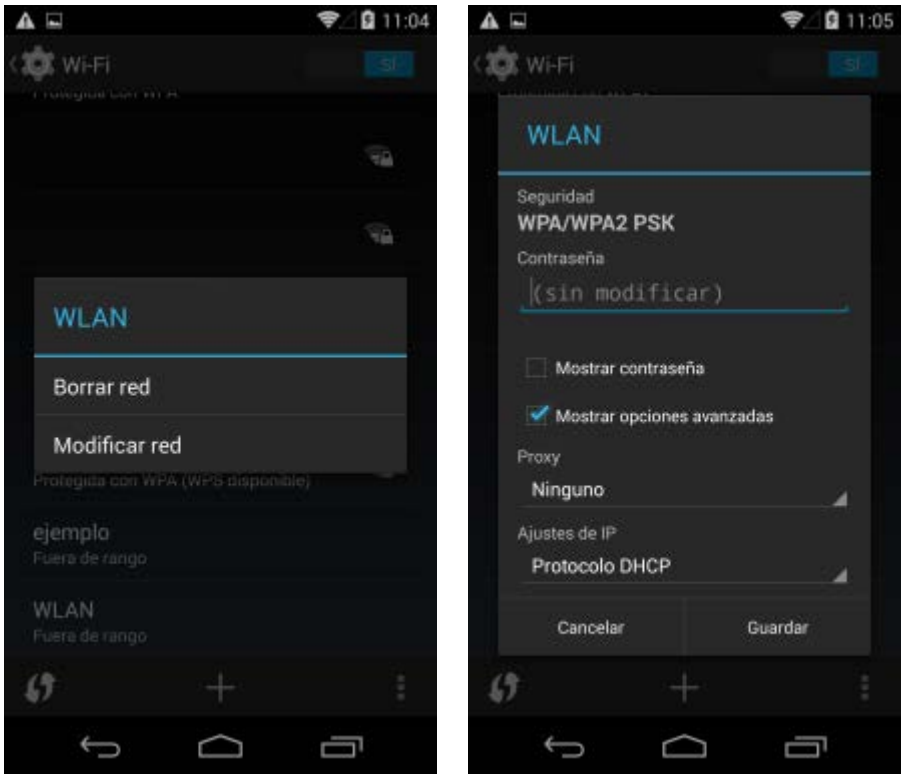
5.17 COMUNICACIONES TCP/IP

925. Esta sección proporciona recomendaciones de seguridad para la pila de comunicaciones TCP/IP del dispositivo móvil, incluyendo recomendaciones generales para TCP/IP (IPv4), SSL/TLS, IPv6 y redes VPN.

5.17.1 ADAPTADORES DE RED

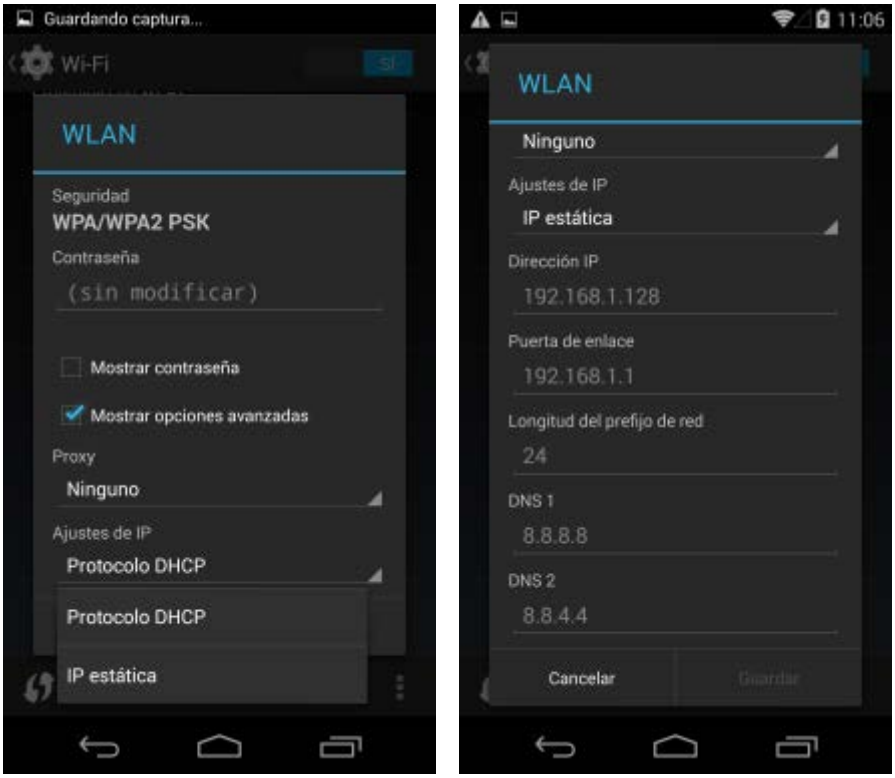
926. La información del adaptador de red disponible en el dispositivo móvil para las comunicaciones mediante tecnologías Wi-Fi (interfaz Wi-Fi) está disponibles desde el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi", una vez se ha establecido una conexión con una red Wi-Fi, mediante una pulsación prolongada sobre dicha red en la lista de redes Wi-Fi disponibles, ya que se mostrará el menú que permite borrar o modificar dicha red.

927. La opción "Modificar red" permite disponer de acceso a la configuración de la red, y mediante la opción "Mostrar opciones avanzadas" es posible visualizar y cambiar la configuración del adaptador de red Wi-Fi:



928. La pantalla de ajustes avanzados permite seleccionar si se utilizará una dirección IP estática o dinámica (DHCP). Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP dinámica obtenida mediante el protocolo DHCP.

929. La configuración de la dirección IP estática permite definir la dirección IP, la puerta de enlace (o router por defecto), la máscara (o prefijo) de red, así como los (dos) servidores DNS:

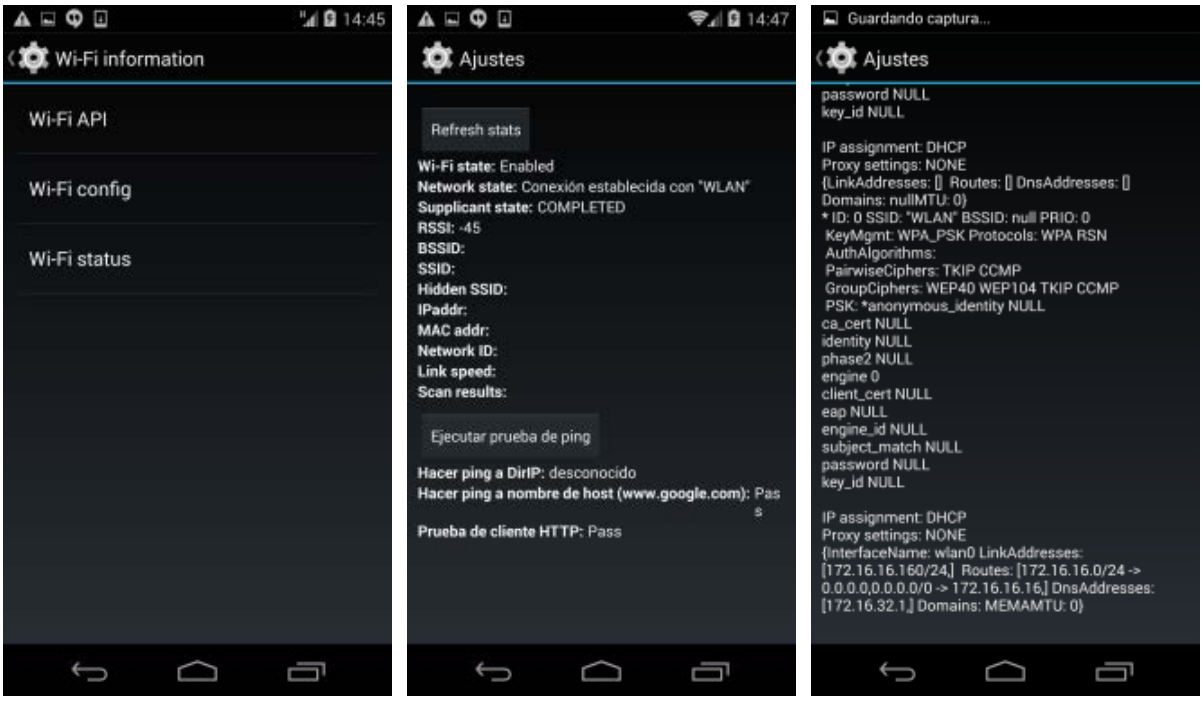


930. La configuración del direccionamiento IP del interfaz Wi-Fi es independiente para cada una de las redes Wi-Fi configuradas (desde la versión 4.0 de Android, "Ice Cream Sandwich"), en lugar de disponerse de una configuración o perfil de red único para todas las red Wi-Fi, tal como ocurría en versiones previas de Android, como 2.x [Ref.- 93].

931. En el caso de emplear una dirección IP asignada dinámicamente por DHCP, es posible obtener información de la misma a través de la entrada correspondiente a la red inalámbrica con la que se ha establecido la conexión Wi-Fi. Desde el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi, se muestra la lista de redes Wi-Fi visibles y aquella a la que estamos conectados.

932. Mediante una pulsación breve sobre dicha red, "dinosec" en el ejemplo, se mostrará una pantalla con los datos de conexión a dicha red, incluyendo la dirección IP que ha sido asignada al dispositivo móvil por el servidor DHCP:

933. Adicionalmente, es posible obtener esta información a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*):

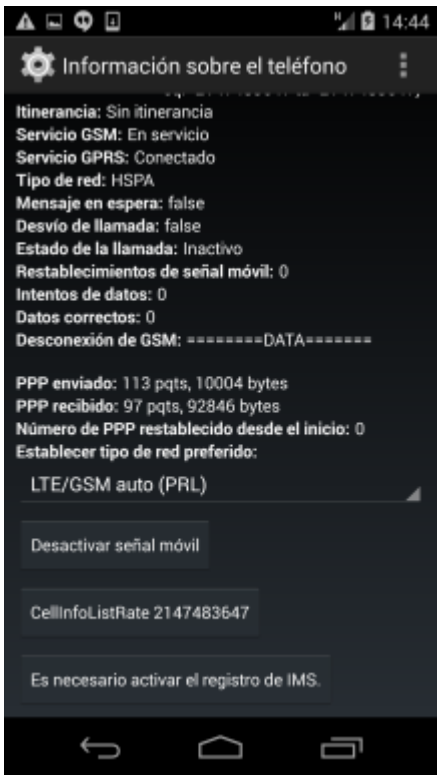


934. La opción "Wi-Fi information - Wi-Fi status", tras pulsar el botón "Refresh stats" en caso de no disponer de datos, proporciona los detalles de conexión de la red Wi-Fi actual, en el ejemplo, red "WLAN" (ver imágenes superiores).

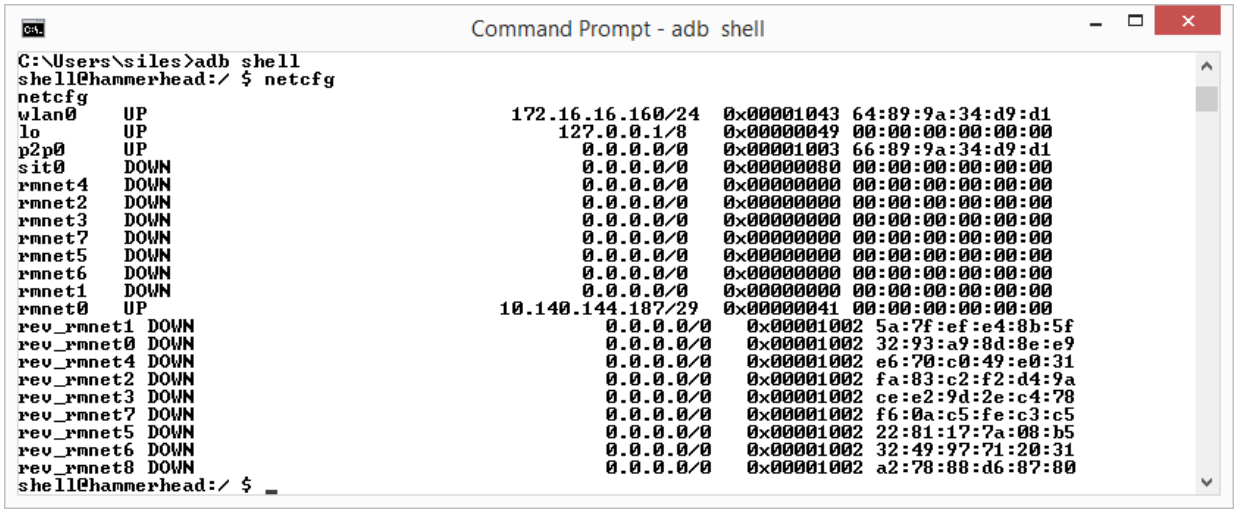
935. Android no proporciona ningún método a través del interfaz de usuario estándar para consultar la dirección IP asignada de forma dinámica por el operador de telefonía móvil al utilizar las redes de datos de telefonía móvil 2/3/4G.

936. De nuevo, es posible obtener esta información a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*).

937. Mediante la selección de la opción "Información sobre el teléfono" se dispone de numerosos detalles de la red de telefonía móvil, y en concreto en la sección inferior denominada "Desconexión de GSM" (en algunos casos) es posible visualizar la dirección IP asignada al dispositivo móvil en el interfaz de datos 2/3/4G ("rmnet0"), junto a las direcciones IP del gateway y de los servidores DNS:



938. Si la información de configuración de TCP/IP para el interfaz de telefonía móvil no es mostrada en dicha sección (depende del modelo de dispositivo móvil y la versión de Android concreta empleada), a través del comando "netcfg" (vía "adb shell") desde un ordenador, es también posible ver la asignación de direcciones IP en ambas redes, red Wi-Fi ("wlan0") y red de telefonía móvil ("rmnet0"):



5.17.2 SEGURIDAD EN TCP/IP

939. Con el objetivo de incrementar el nivel de seguridad de la pila TCP/IP empleada para las conexiones de datos en Android, se recomienda evaluar su comportamiento y (de ser posible) modificar ciertos parámetros de configuración que condicionan su funcionamiento y nivel de seguridad.

940. Se recomienda deshabilitar el procesamiento de paquetes de *ping*, es decir, paquetes ICMP *echo request* entrantes y sus respuestas asociadas, paquetes ICMP *echo response* salientes, con el objetivo de limitar el descubrimiento del dispositivo móvil en la red (habilitados por defecto en Android).

Nota: no se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar el procesamiento de paquetes de *ping*, es decir, la recepción de paquetes *ICMP echo request* y sus respuestas asociadas, *ICMP echo response*.

Igualmente, no se han encontrado mecanismos que permitan modificar los diferentes parámetros de configuración de bajo nivel de la pila TCP/IP mencionados en este apartado.

941. Android también responde a otros tipos de mensajes ICMP de petición y respuesta, como por ejemplo ICMP *timestamp*, aunque no responde a mensajes ICMP *address subnet mask*.

942. La identificación del dispositivo móvil también se puede llevar a cabo a través del protocolo DHCP, ya que en las peticiones DHCP (DHCP *Discover* y *Request*) Android incluye varios datos identificativos.

943. Las peticiones de Android añaden la opción 60 de DHCP, identificación del vendedor (*Vendor class identifier*), con el mensaje "dhcpcd-5.5.6", es decir, hace uso del cliente DHCP estándar de Linux DHCPCD (DHCP Client Daemon), versión 5.5.6.

944. La última versión disponible de dhcpcd para Linux en el momento de elaboración de la presente guía es la 6.7.1 [Ref.- 48].

Nota: en septiembre de 2014 se publicó una vulnerabilidad de denegación de servicio (DoS) en dhcpcd que afectaba a todas las versiones desde la 4.0.0 hasta la 6.4.2. Se confirmó que la versión 5.5.6 de dhcpcd disponible en Android 4.4.4 es vulnerable, estando solucionada esta vulnerabilidad en Android 5.0 (Lollipop) [Ref.- 192]. Más información:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6060
http://roy.marples.name/projects/dhcpcd/ci/1d2b93aa5ce25a8a710082fe2d36a6bf7f5794d5?sbs=0

945. Las peticiones también incluyen la opción 12 de DHCP, nombre de equipo (*Host Name*), con el valor "android_CÓDIGO", dónde "CÓDIGO" es un string de 16 caracteres hexadecimales correspondiente al ANDROID_ID (asociado a la propiedad "net.hostname"; ver apartado "5.9. Configuración por defecto del dispositivo móvil").

946. Adicionalmente, por defecto el dispositivo móvil Android envía peticiones NTP (*Network Time Protocol, UDP/123*) para su sincronización horaria hacia servidores NTP disponibles en Internet periódicamente.

5.17.3 ESCANEO DE PUERTOS TCP Y UDP

947. A continuación se analiza el comportamiento de la pila TCP/IP de Android frente a intentos de conexión TCP y UDP a través del interfaz Wi-Fi. El análisis se ha realizado en la configuración por defecto del dispositivo móvil, es decir, sin haber realizado ninguna configuración específica o instalación adicional de software.

948. Android responde con un paquete TCP *Reset* a las peticiones de conexión hacia puertos TCP cerrados.

949. Por defecto, Android no dispone de ningún puerto TCP abierto o filtrado, es decir, los 65.536 puertos TCP están cerrados.

950. Android responde con paquetes ICMP de tipo 3 y código 3 (destino inalcanzable, puerto inalcanzable), limitados a uno por segundo, a las peticiones de conexión hacia puertos UDP cerrados.

951. Por defecto, Android no dispone de ningún puerto UDP abierto, tanto si DHCP está configurado en el interfaz Wi-Fi como cuando se utiliza una dirección IP estática.

952. El comportamiento por defecto de la pila TCP/IP, y especialmente la ausencia de mecanismos de filtrado de tráfico (cortafuegos personal) y sus peculiaridades a nivel de TCP y UDP, podrían hacer posible la identificación de los dispositivos móviles basados en Android.

953. Este tipo de identificación remota a través de la red facilitaría a un potencial atacante la realización de ataques dirigidos sobre vulnerabilidades conocidas, por lo que se enfatiza la necesidad de mantener el software del dispositivo móvil completamente actualizado en todo momento.

Nota: el comportamiento de la pila TCP/IP frente a escaneos de puertos a través del interfaz de telefonía móvil de datos (cuando está conectado a la red real del operador) no puede ser analizado de forma fiable. Este comportamiento a través del interfaz de telefonía móvil de datos está condicionado por la infraestructura de comunicaciones y los mecanismos de filtrado de los operadores de telefonía móvil, que por ejemplo, pueden no permitir comunicaciones mediante ping (*ICMP echo request* y *reply*) o pueden disponer de *proxies* transparentes en la red, por ejemplo para protocolos como FTP o HTTP.

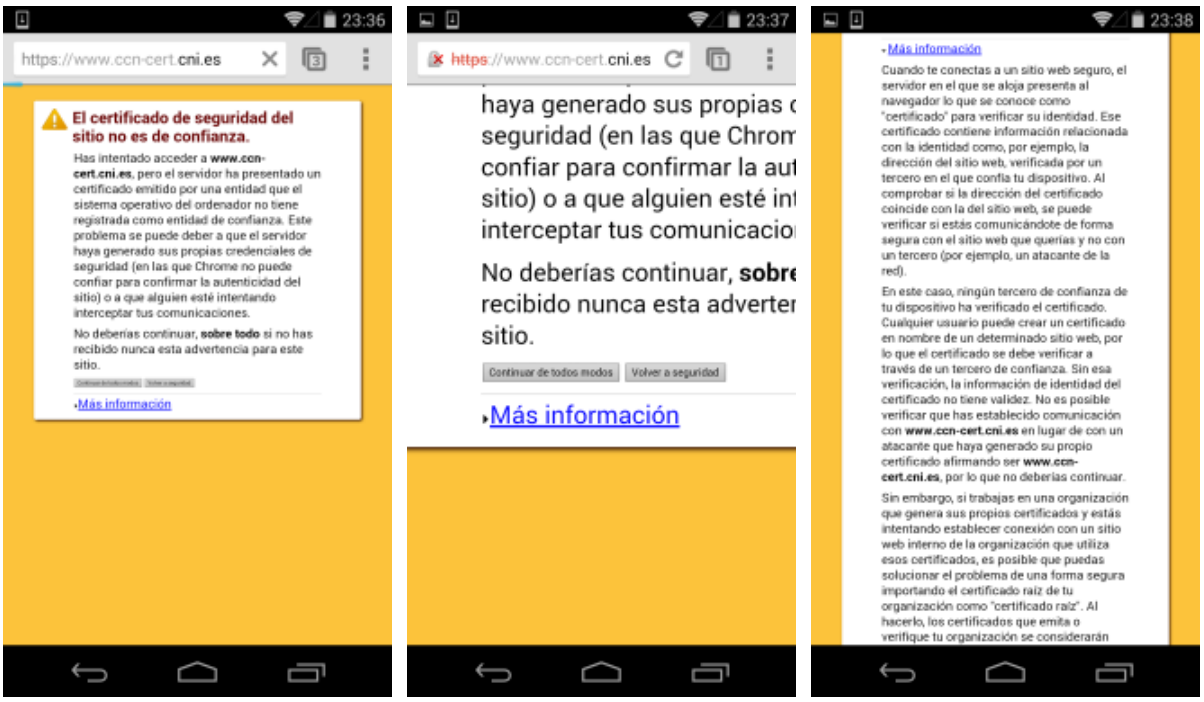
5.17.4 SSL/TLS

954. Android dispone de una implementación de los protocolos SSL, Secure Socket Layer, y TLS, Transport Layer Security, a través del paquete Java denominado "javax.net.ssl", con soporte para SSL v3.0 y hasta TLS v1.2, basado (parcialmente) en la implementación de *The Legion of the Bouncy Castle* y de OpenSSL [Ref.- 99].

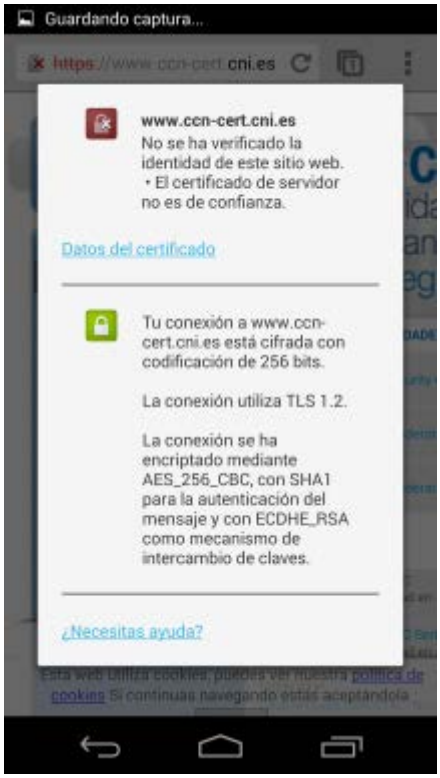
955. Al acceder a un sitio web mediante HTTPS utilizando el navegador web existente en Android por defecto (app "Chrome" en Android versión 4.x), el dispositivo móvil intentará

verificar el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (CA, *Certificate Authority*) raíz reconocida correspondiente.

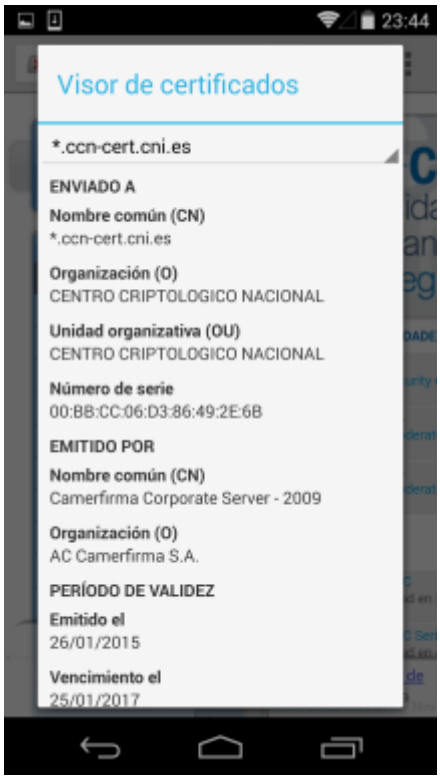
956. En caso de que no sea posible verificar la validez de un certificado, el navegador web de Android generará un mensaje de advertencia, indicando el motivo del error y permitiendo al usuario ver y analizar algunos detalles del motivo a través del enlace "Más información":

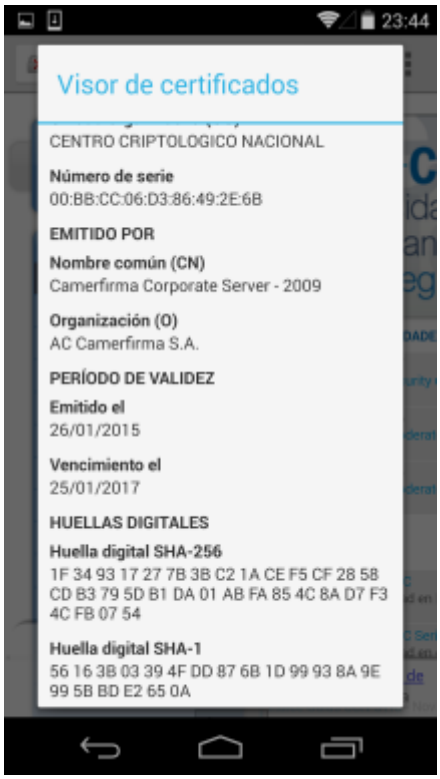


957. Sin embargo, la información detallada del certificado digital obtenido no está directamente disponible. Es necesario pulsar el botón "Continuar de todos modos", y establecer la conexión no verificada mediante HTTPS con el servidor web, para poder pulsar en el icono del candado (con una cruz roja) disponible en la barra de navegación o URL, y así poder obtener los detalles del certificado digital:



958. La pantalla proporciona, en su parte inferior, detalles de la conexión SSL/TLS y los algoritmos y parámetros negociados entre el navegador web y el servidor web. El enlace "Datos del certificado" permite obtener los detalles del certificado digital a través del "Visor de certificados", que incluye elementos clave para su verificación, como por ejemplo el número de serie del certificado, las huellas o *fingerprints* SHA-1 o SHA-256, información de la autoridad certificadora involucrada en su emisión, etc:





959. Si se acepta un certificado digital, éste será válido hasta que se cierre la instancia, proceso, o sesión actual del navegador web en Android.

960. Esta aceptación tiene el riesgo asociado de que el certificado digital aceptado, y desconocido, puede pertenecer a un potencial intruso que se encuentra realizando un ataque de intercepción del tráfico del usuario, MitM (Man-in-the-Middle), sobre el protocolo SSL/TLS y las comunicaciones (supuestamente) cifradas.

961. Como se describe en el apartado "5.7. Gestión de certificados digitales y credenciales en Android", en Android 4.x el repositorio de certificados raíz está accesible a través del interfaz de usuario de Android. Por tanto, el usuario puede gestionar la lista autoridades certificadoras (o CAs, *Certificate Authorities*) que son consideradas de confianza por Android.

962. Android desde la versión 4.0 (Ice Cream Sandwich) soporta la utilización de mecanismos de autentificación web basados en certificados digitales cliente a través del navegador web existente por defecto [Ref.- 117], al igual que es posible hacer uso de certificados cliente para la conexión a redes Wi-Fi o redes VPN (ver apartado "5.7. Gestión de certificados digitales y credenciales en Android").

963. La funcionalidad para el uso de certificados digitales cliente en el navegador web añadida finalmente en Android versión 4.0 [Ref.- 118] permite gestionar (visualizar, deshabilitar, habilitar, instalar, eliminar, etc.) las CAs desde el interfaz de usuario de Android y la sección "Ajustes - Seguridad", así como gestionar certificados digitales cliente para el dispositivo móvil y las apps (como el navegador web o los clientes de correo electrónico) a través de un nuevo KeyChain (o gestor de credenciales y certificados) [Ref.- 119] [Ref.- 185].

964. Previamente se disponía de un gestor de credenciales y certificados global para todo el sistema pero únicamente accesible para la conexión a redes Wi-Fi y VPN, a través de "Ajustes" [Ref.- 185]. Las apps debían hacer uso de sus propios gestores de certificados privados, ya que no disponían de una API para acceder a los certificados existentes en el repositorio del sistema.

965. En Android 4.x, los certificados digitales cliente guardados en el repositorio de credenciales están disponibles para su utilización por parte del navegador web [Ref.- 182].

966. Existen otros navegadores web de terceros (como por ejemplo Firefox para Android, junto al *add-on* o extensión Cert Manager[88], SandroB, etc.), que también disponen de capacidades de autentificación web basada en certificados digitales cliente, y que adicionalmente definen su propio gestor de certificados cliente (KeyManager) y su propio gestor de confianza (TrustManager, para gestionar sus propias CAs) a través de "javax.net.ssl.SSLContext".

5.17.5 IPV6

967. El protocolo IP versión 6 (IPv6) está soportado y activado por defecto en Android para las comunicaciones de datos mediante Wi-Fi y telefonía móvil 2/3/4G.

968. En Android 4.4 (KitKat) el usuario dispone de capacidades para visualizar la información de las direcciones IPv6 a través del menú "Ajustes - Información del teléfono - Estado", y

[88] https://addons.mozilla.org/en-US/mobile/addon/cert-manager/

en concreto, en el campo "Dirección IP"[89], aunque no dispone de ninguna opción de configuración relacionada con IPv6 desde el interfaz gráfico de usuario (o GUI):

Nota: la disponibilidad de IPv6 para las comunicaciones de datos a través de la infraestructura de telefonía móvil en Android es dependiente tanto de la versión del sistema operativo, como del modelo de dispositivo móvil y del operador de telefonía móvil empleados [Ref.- 54].

969. Por otro lado, y desde el punto de vista de la funcionalidad, es necesario evaluar si Android soporta únicamente redes de datos basadas en IPv6, sin hacer uso de la pila TCP/IP versión 4 [Ref.- 57]. Las redes de telefonía móvil 2/3/4G basadas sólo en IPv6 están soportadas por Android, y las redes Wi-Fi también lo están, aunque inicialmente con problemas conocidos de conectividad relacionados con la coexistencia de IPv6 e IPv4.

970. Para disponer de conectividad IPv6 completa en Android y obtener una dirección IPv6 a través de mensajes RA (Router Advertisement) enviados por un router con soporte de IPv6 es necesario que el interfaz Wi-Fi disponga también de dirección IPv4 (estática o mediante DHCP).

971. Es posible forzar el uso exclusivo de IPv6 en el interfaz Wi-Fi de Android, y evitar los problemas conocidos mencionados, estableciendo una dirección IP fija para la red Wi-Fi igual a 0.0.0.0, el mismo valor que también debe ser asignado al *gateway* [Ref.- 57].

Nota: las limitaciones del uso exclusivo de IPv6 en el interfaz Wi-Fi de Android están relacionadas también con problemas en el soporte para otras funcionalidades de IPv6:
- RFC3315 (DHCPv6): https://code.google.com/p/android/issues/detail?id=32621
- RFC6106 (RDNSS): https://code.google.com/p/android/issues/detail?id=32629 [90]

[89] https://plus.google.com/+KevinOtte/posts/JUHVxyW1AB3
[90] Resuelto en Android 5.0 (Lollipop): https://code.google.com/p/android/issues/detail?id=32630

972. Durante el proceso de inicialización de conectividad de datos, el dispositivo móvil Android genera peticiones IPv6 de solicitud de vecinos y de router mediante ICMPv6, empleando como dirección origen "fe80::6689:9aff:fe01:0203" (dónde su dirección MAC es 64:89:9a:01:02:03), y añadiendo también su dirección MAC como dirección de enlace.

973. La utilización de la dirección MAC en la dirección IPv6 sin hacer uso de las Privacy Extensions de IPv6 (RFC 4941) presenta problemas de seguridad y permite el seguimiento de los dispositivos móviles Android en Internet [Ref.- 55].

974. Finalmente, Android 4.0 añadió soporte para las Privacy Extensions de IPv6, pero sin capacidades de configuración , ya que su utilización está configurada por defecto, pero no puede ser deshabilitada en caso de que sea necesario (aunque no recomendado desde el punto de vista de seguridad) [Ref.- 59].

975. Adicionalmente, el dispositivo móvil Android envía periódicamente mensajes IPv6 de informes multicast ("Multicast Listener Report Message v2").

976. Se recomienda deshabilitar la disponibilidad de IPv6 en Android por completo, salvo que se vaya hacer uso de sus capacidades de comunicación, aunque esta opción no está disponible actualmente en la versión de Android analizada (salvo en dispositivos Android *rooted*).

Nota: no se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar o gestionar la pila de comunicaciones de IPv6.

5.17.6 REDES VPN

977. Android, desde la versión 4.0 (Ice Cream Sandwich), proporciona soporte para las siguientes tecnologías y protocolos empleados por redes VPN (*Virtual Private Networks*, o redes privadas virtuales) [Ref.- 21]:

- PPTP: Point-to-Point Tunneling Protocol (TCP/1723).
- L2TP/IPSec: Layer Two Tunneling Protocol (L2TP; UDP/1701) en combinación con Internet Protocol Security (IPSec; protocolos IP 50 y 51 + IKE: UDP/500).
    - L2TP/IPSec PSK
    - L2TP/IPSec RSA
- IPSec: Internet Protocol Security (protocolos IP 50 y 51 + IKE: UDP/500).
    - IPSec Xauth PSK
    - IPSec Xauth RSA[91]
    - IPSec Hybrid RSA[92]

978. La opción recomendada desde el punto de vista de seguridad es hacer uso de redes VPN basadas en IPSec o L2TP/IPSec.

979. Desde el punto de vista de seguridad no se recomienda hacer uso de redes VPN basadas en PPTP, ya que este protocolo hace uso de MSCHAPv2 para el proceso de autentificación, y

[91] http://tools.ietf.org/html/draft-ietf-ipsec-isakmp-xauth
[92] http://tools.ietf.org/html/draft-ietf-ipsec-isakmp-hybrid-auth

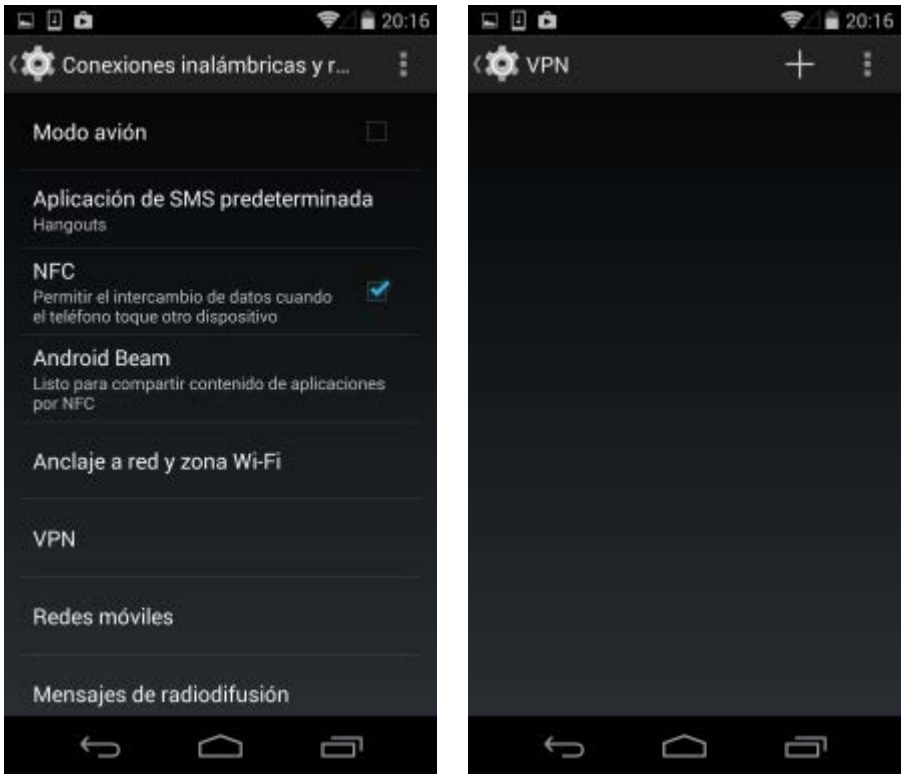
éste es vulnerable a ataques de fuerza bruta con un 100% de éxito (representado por la totalidad de posibilidades asociadas a una clave DES, es decir, 2^{56}) [93].

980. Adicionalmente, en el caso hacer uso de redes VPN basadas en L2TP/IPSec o IPSec, se debe definir el método de autentificación a emplear: certificados digitales (opción "RSA") o clave precompartida (opción "PSK", *Pre-Shared Key*).

981. Se recomienda emplear certificados para la autentificación de L2TP/IPSec o IPSec al ser un mecanismo más seguro que el establecimiento de una clave precompartida (PSK) entre el servidor de VPN y el dispositivo móvil (que además es conocida por todos los usuarios de la red VPN y puede ser usada en ataques MitM[94]).

982. En el caso de IPSec Xauth RSA tanto el cliente como el servidor se autentifican inicialmente empleando certificados digitales durante la fase 1 de IKE (autentificación mutua). Posteriormente, el cliente se autentifica de nuevo mediante Xauth (ej. usuario y contraseña). En el caso de IPSec Hybrid RSA el cliente no se autentifica durante la fase 1 de IKE, sino que sólo verifica que está hablando con el servidor legítimo, lo que simplifica el despliegue de la solución VPN al no ser necesaria la emisión de certificados digitales cliente, pero constituye una solución más robusta que IPSec Xauth PSK. Posteriormente, de nuevo, el cliente se autentifica mediante Xauth (ej. usuario y contraseña).

983. Desde el menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN" es posible añadir una nueva red VPN a través del botón con el símbolo "+" de la parte superior:

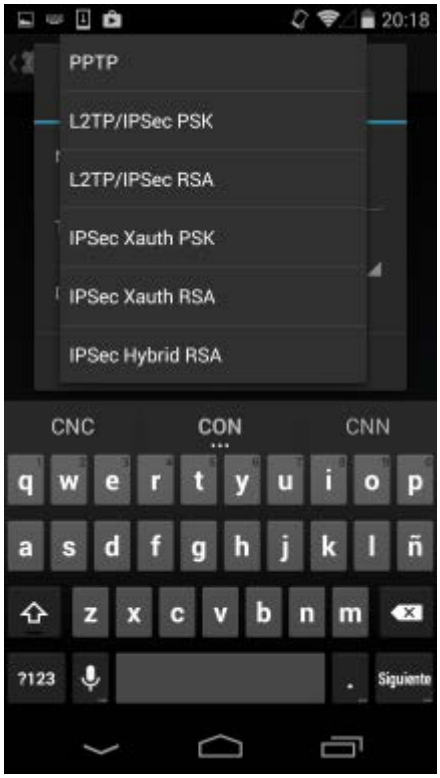


984. A través de las diferentes opciones disponibles asociadas al perfil de la red VPN es posible configurar todos los detalles de la conexión VPN. Una vez se han establecido las opciones de configuración según el tipo de red (descritas a continuación), mediante el botón "Guardar" es posible almacenar la nueva configuración.

[93] https://www.cloudcracker.com/dictionaries.html
[94] http://www.cisco.com/en/US/tech/tk583/tk372/technologies_security_notice09186a0080215981.html

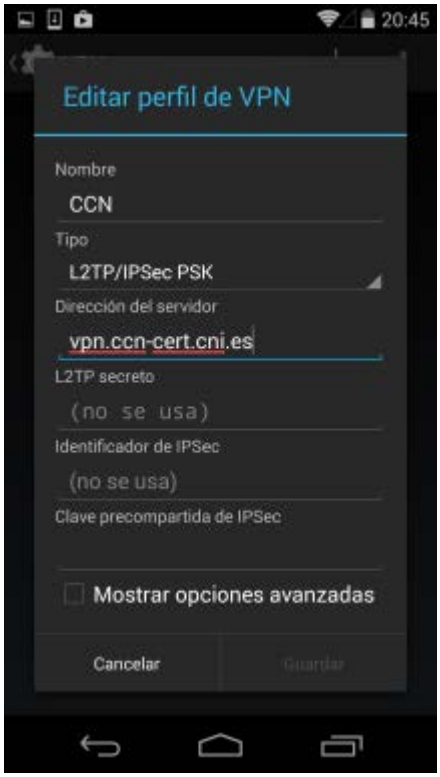
985. Todas las redes VPN, basadas en PPTP, L2TP/IPSec e IPSec, requieren disponer del nombre de la red VPN, del tipo de red VPN y del nombre o dirección IP del servidor VPN.

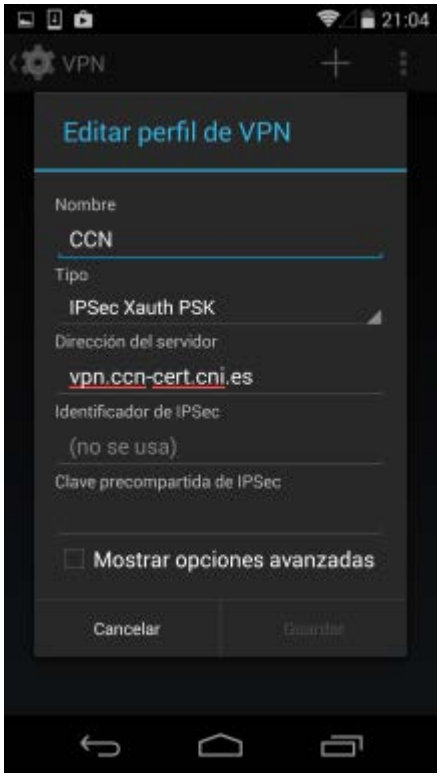
986. En el caso de redes PPTP, Android permite deshabilitar el cifrado mediante la opción "Encriptación de PPP (MPPE)", que está habilitada por defecto. Se desaconsejada deshabilitar este mecanismo de cifrado desde el punto de vista de seguridad:



987. La opción "Mostrar opciones avanzadas" permite especificar los dominios de búsqueda de DNS, los servidores DNS, y posibles rutas para el envío del tráfico de red, es decir, modificar elementos relacionados con la pila TCP/IP de Android y, en concreto, con la resolución de nombres (DNS) y la tabla de enrutamiento de Android:

988. En el caso de redes L2TP/IPSec PSK, y de redes IPSec Xauth PSK, Android permite establecer la clave precompartida para el acceso a la red:





989. Tanto para redes L2TP/IPSec PSK como RSA, Android, en función del tipo de red VPN, también permite habilitar un secreto L2TP (deshabilitado por defecto), opción que facilita autentificar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (y que puede ser necesario en función de la configuración del servidor VPN).

990. En el caso de redes L2TP/IPSec RSA, y de redes IPSec Xauth RSA, Android permite establecer el certificado digital cliente de usuario de IPSec, el certificado de la autoridad certificadora (CA) que ha emitido el certificado del servidor o concentrador VPN, y específicamente, el certificado digital del servidor o concentrador VPN (si no se especifica un certificado digital concreto, Android por defecto aceptará el certificado recibido al establecer la conexión, opción desaconsejada desde el punto de vista de seguridad):

991. Por defecto, Android no obliga a que la configuración de la red VPN basada en L2TP/IPSec RSA verifique el certificado de la CA que ha emitido el certificado del servidor o concentrador VPN.

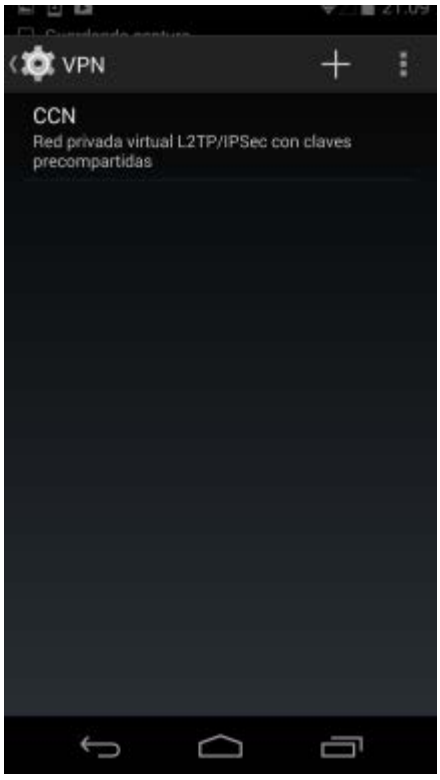
992. Esta es la opción desaconsejada desde el punto de vista de seguridad, ya que al no verificar la CA, se permite que un potencial atacante suplante al servidor o concentrador VPN y se haga pasar por el servidor legítimo. En su lugar, siempre se debe seleccionar el certificado digital de la CA que está siendo empleado por la red VPN, y que debe haber sido importado previamente en el almacén de certificados de Android (ver apartado "5.7. Gestión de certificados digitales y credenciales en Android").

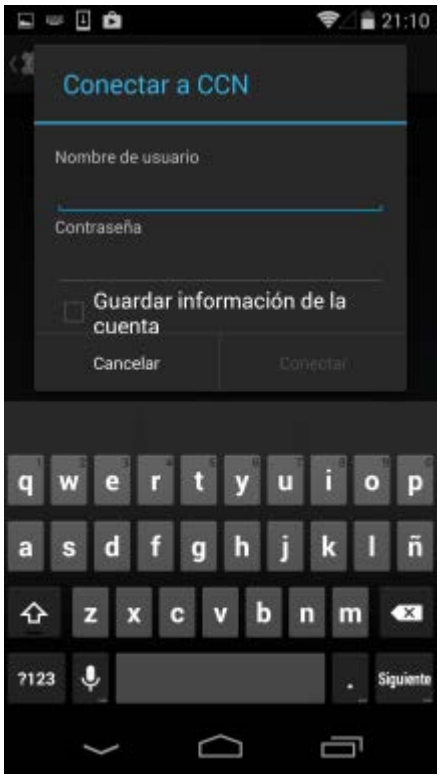
993. El certificado digital cliente necesario para L2TP/IPSec es de tipo personal, y permitirá autentificar al dispositivo móvil y a su propietario. Adicionalmente, como se ha recomendado previamente, es necesario instalar un certificado raíz (perteneciente a la CA), y asociado a la generación del certificado digital empleado por el servidor de la red VPN.

994. En el caso de redes L2TP/IPSec basadas en certificados digitales, al seleccionar el certificado cliente del usuario y de la CA, Android mostrará los certificados disponibles en el repositorio de credenciales, previamente importados (ver apartado "5.7. Gestión de certificados digitales y credenciales en Android").

995. En el caso de redes IPSec Hybrid RSA se pueden definir los certificados de la CA y del servidor o concentrador VPN, pero no se hace uso de un certificado digital cliente ni de una clave precompartida (opciones Xauth previas).

996. Una vez configurada la red VPN, es posible conectarse a la misma seleccionándola de la lista de redes disponibles desde la pantalla "Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN", mediante una pulsación corta sobre la misma:





997. Como resultado, Android solicitará al usuario las credenciales de acceso a la red VPN, es decir, el nombre de usuario y la contraseña para establecer la conexión con la red VPN seleccionada.

998. Desde el punto de vista de seguridad se recomienda no seleccionar la opción "Guardar información de la cuenta", ya que si no, se almacenarán las credenciales de acceso a la red VPN en el dispositivo móvil. Es preferible que cada vez que se establezca una conexión con una red VPN sea necesario proporcionar tanto el usuario como la contraseña.

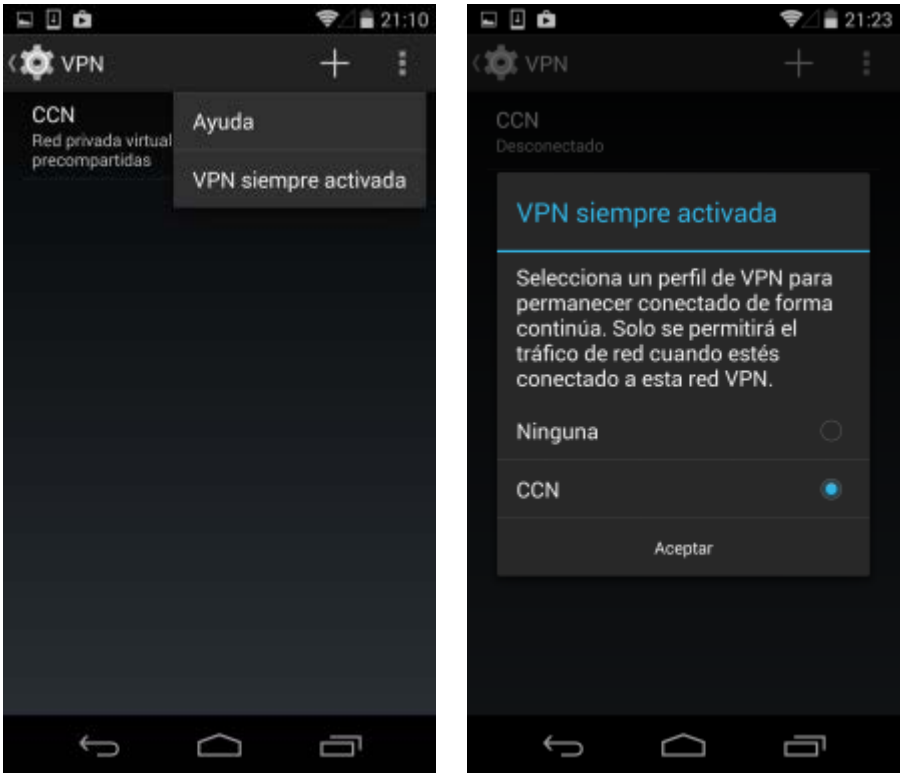
999. En el caso de dispositivos móviles Android multiusuario, únicamente el usuario propietario (o usuario principal) puede modificar la configuración de las redes VPN.

1000. Una vez establecida la conexión con la red VPN, Android restringe las comunicaciones para que todo el tráfico sea cursado a través de la red VPN hasta que el dispositivo móvil se desconecte de ella, es decir, no soporta *split horizon* (conexiones simultáneas directas hacia Internet y a través de la red VPN).

1001. Una vez se ha establecido la conexión con la red VPN, aparecerá un icono con forma de llave en la barra superior de estado y se añadirá una notificación al centro de notificaciones. Para desconectarse de la red VPN, el usuario sólo debe seleccionar dicha notificación, correspondiente a la red VPN activa.

1002. Mediante una pulsación prolongada sobre la red VPN, desde la lista de redes disponibles en la pantalla "Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN", es posible editar o eliminar el perfil de la red VPN:

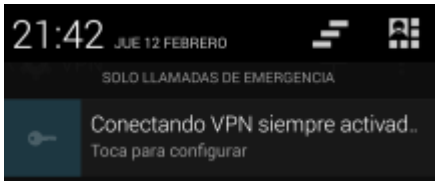
1003. Adicionalmente, si la red VPN lo permite, Android dispone de la posibilidad, a través del botón de menú disponible en la parte superior ("...") y de la opción "VPN siempre activada", de forzar que no sea posible cursar ningún tráfico de red (ni recibir, ni enviar) si la conexión a la red VPN no está establecida [Ref.- 21]:



1004. Esta es la opción recomendada desde el punto de vista de seguridad, ya que permite asegurar que no se enviará tráfico no cifrado y potencialmente sensible a través de la red, ya sea la red de datos de telefonía móvil 2/3/4G o una red Wi-Fi.

1005. Para poder hacer uso de esta funcionalidad, sí es necesario seleccionar la opción "Guardar información de la cuenta" (desaconsejada previamente, salvo que se haga uso de esta funcionalidad), con el objetivo de que el dispositivo móvil disponga en todo momento de las credenciales del usuario para el acceso a la red VPN y pueda restablecer la conexión automáticamente en caso de ser necesario, por ejemplo, porque se hay interrumpido la conexión temporalmente.

1006. Adicionalmente, para poder hacer uso de esta funcionalidad, Android también requiere que se especifique una dirección IP (en lugar de un nombre) para el servidor o concentrador de la red VPN y para el servidor DNS:



1007. El modo "VPN siempre activada" puede ser desactivado a través de la opción "Ninguna".

1008. Por último, Android no dispone de soporte nativo para redes VPN basadas en OpenVPN, siendo necesario instalar una app de terceros que actúe de cliente OpenVPN para este tipo de conexiones, como por ejemplo el cliente oficial de OpenVPN para Android disponible en Google Play[95].

5.18 CUENTA DE USUARIO DE GOOGLE

1009. Para hacer uso de las apps de Google en Android (Gmail, Google+, Fotos, Maps, Contactos, Calendario, Drive, YouTube, etc.) y especialmente de toda su funcionalidad, además de poder descargar aplicaciones de Google Play [Ref.- 4] (ver apartado "5.22.4. Apps de terceros: Google Play"), hacer copias de seguridad de los datos y la configuración en los servidores de Google (ver apartado "5.20.2. Copia de seguridad en los servidores de Google"), y poder hacer uso de otros servicios de Google desde el dispositivo móvil, es necesario disponer de una cuenta de usuario de Google:

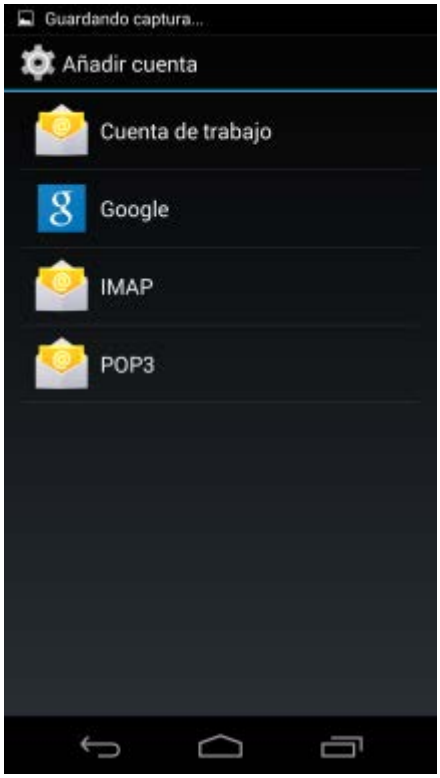
[95] https://play.google.com/store/apps/details?id=net.openvpn.openvpn

1010. Entre otros, los siguientes servicios de Google están disponibles para los usuarios de Android 4.x: Gmail, Google+, Fotos, Maps, Contactos, Calendario, Keep, Drive, YouTube, Hangouts, etc.

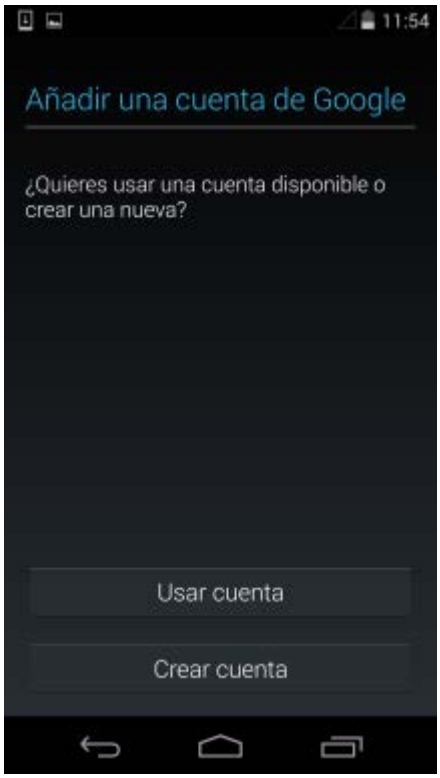
5.18.1 ASIGNACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE AL DISPOSITIVO MÓVIL

1011. La configuración de una cuenta de usuario de Google ya existente y su vinculación al dispositivo móvil Android, o la creación de una nueva cuenta, puede llevarse a cabo mediante el proceso de de instalación y configuración inicial de Android 4.x (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial").

1012. Asimismo, una vez el dispositivo móvil ha sido configurado, puede vincularse a una cuenta de usuario de Google desde el menú "Ajustes [Cuentas]". El botón "Añadir cuenta" permite añadir tanto una cuenta de usuario de Google, como cuentas de usuario de distintos tipos, como por ejemplo de Microsoft Exchange , identificadas mediante la opción "Cuenta de trabajo", y cuentas de correo electrónico IMAP y POP3, siendo necesario proporcionar las credenciales de la cuenta existente, es decir, la dirección de correo electrónico del usuario y la contraseña (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android"):



1013. En el caso de las cuentas de usuario de Google, es posible seleccionar si se añadirá una cuenta ya existente (para lo que se solicitarán las credenciales de acceso) o se creará una nueva cuenta (siendo posible asociar múltiples cuentas al dispositivo móvil):

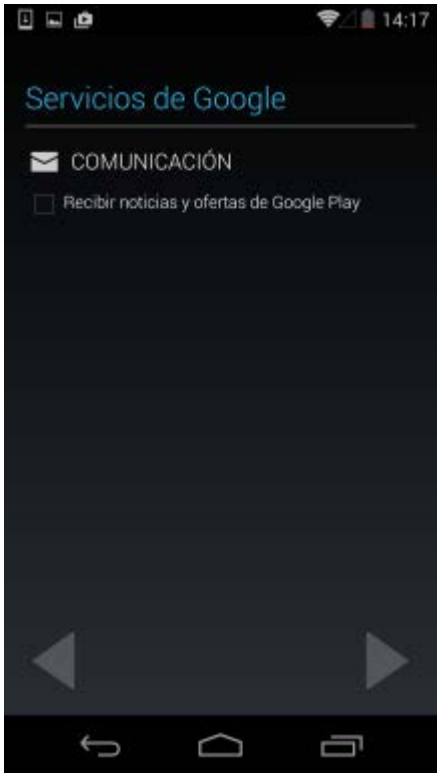


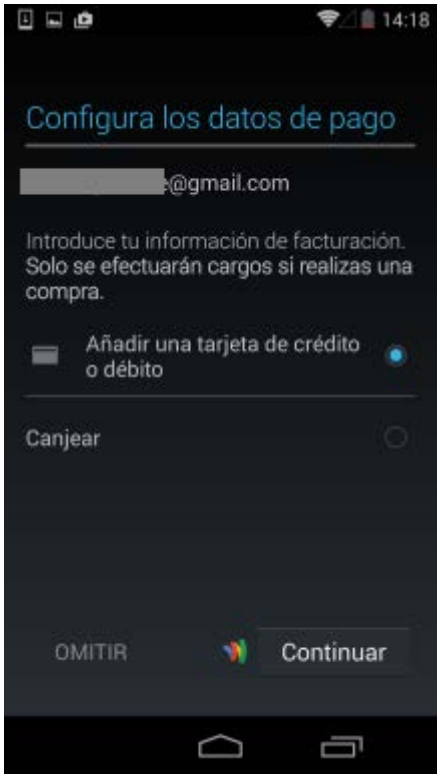
1014. Tanto el botón "Usar cuenta", como el botón "Crear cuenta", redirigirán al usuario a la configuración del interfaz Wi-Fi y lo activarán (incluso aunque estuviera apagado previamente), con el objetivo de disponer de conexión a Internet y poder hacer uso de la cuenta de usuario de Google ya existente, o permitir la creación de una cuenta nueva.

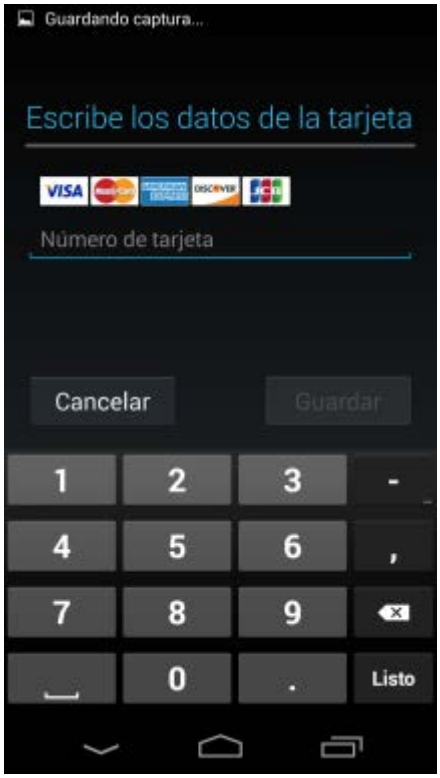
1015. Es importante tener en consideración este matiz si no se desea que se active el interfaz Wi-Fi de manera automática en la ubicación actual.

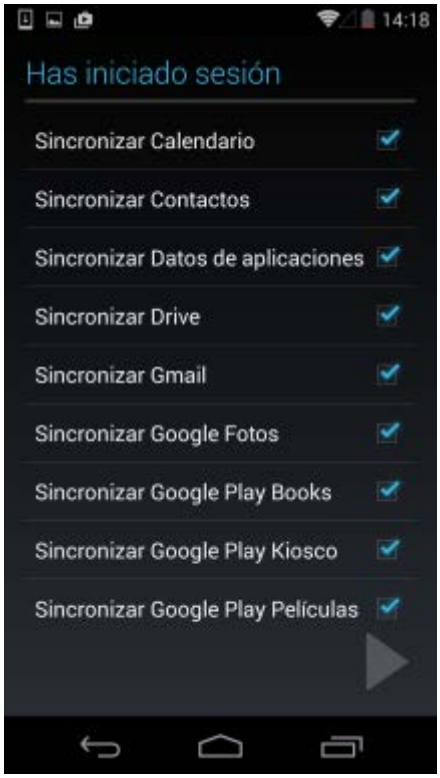
1016. Adicionalmente, para configurar y poder hacer uso de otros servicios críticos y relevantes en Android, como por ejemplo el acceso a Google Play y a apps de terceros (ver apartado "5.22.4. Apps de terceros: Google Play"), es también necesario disponer de una cuenta de usuario de Google.

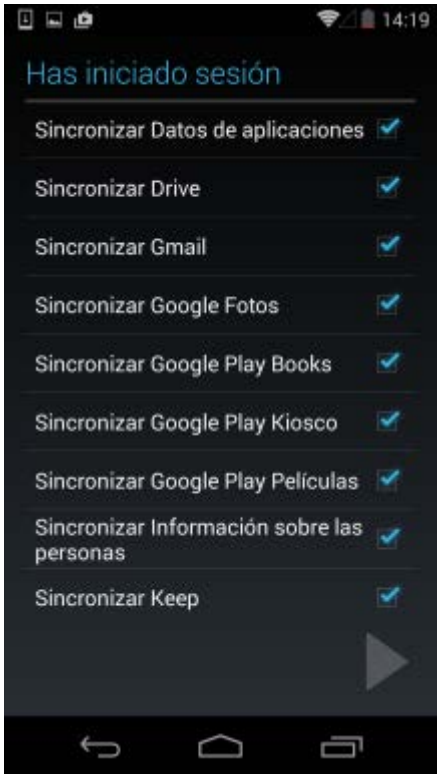
1017. El proceso de vinculación de una cuenta de usuario de Google existente se lleva a cabo mediante una conexión HTTPS inicial con el servidor "www.googleapis.com" (entre otros). Durante el mismo se solicita confirmación por parte del usuario para hacer uso de los servicios de Google+, comunicaciones (noticias y ofertas de Google Play), configurar los datos de pago (fuera del alcance de la presente guía), y definir los servicios que serán sincronizados entre el dispositivo móvil y Google, todos ellos habilitado por defecto:



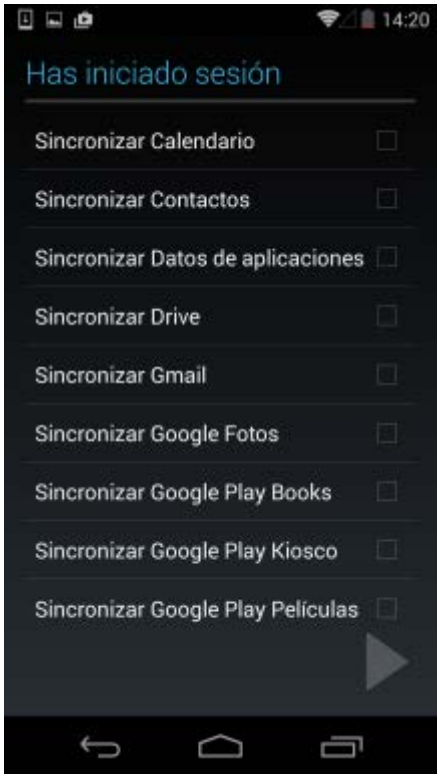


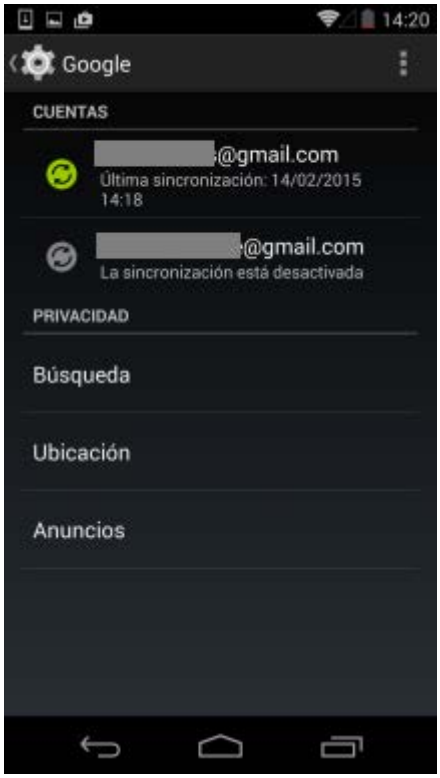






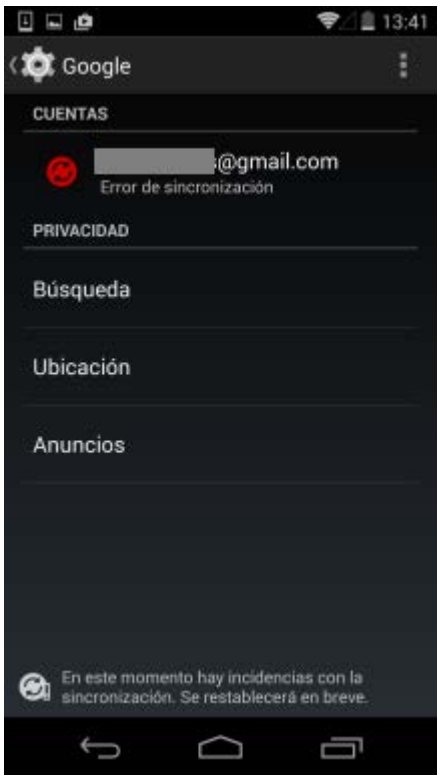
1018. Una vez se ha vinculado una cuenta de usuario de Google con el dispositivo móvil, se realizará la sincronización automática, siendo posible no llevar a cabo (o cancelar) esta sincronización inicial deshabilitando todos los servicios listados, escenario reflejado por el mensaje "La sincronización está deshabilitada" bajo el nombre de cuenta de usuario de Google:



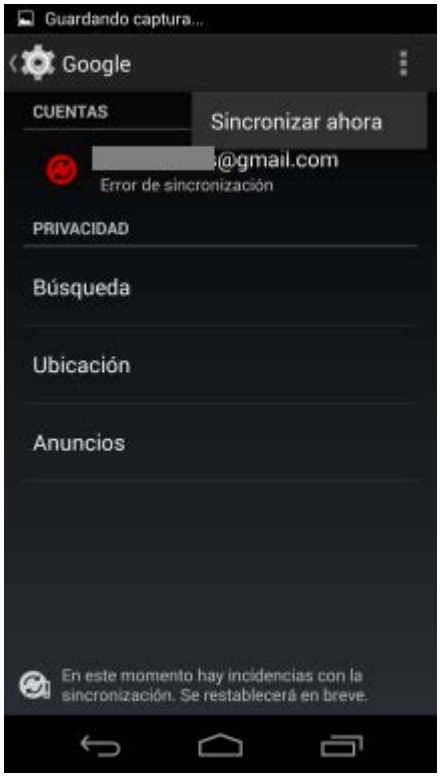


1019. La sincronización de las cuentas de Google es bidireccional, es decir, los cambios del dispositivo móvil se reflejarán en los servicios web de Google, y viceversa.

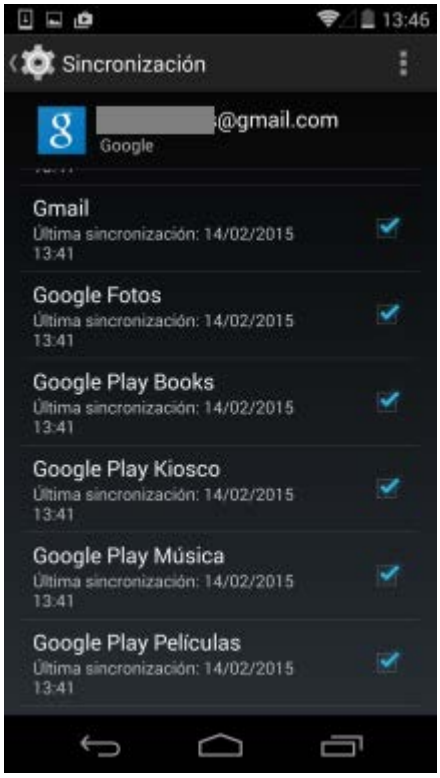
1020. Adicionalmente, una vez vinculada, la cuenta de usuario de Google aparecerá en el menú "Ajustes - [Cuentas]" una nueva entrada denominada "Google", que permite el acceso a los detalles de las cuentas de usuario de Google:

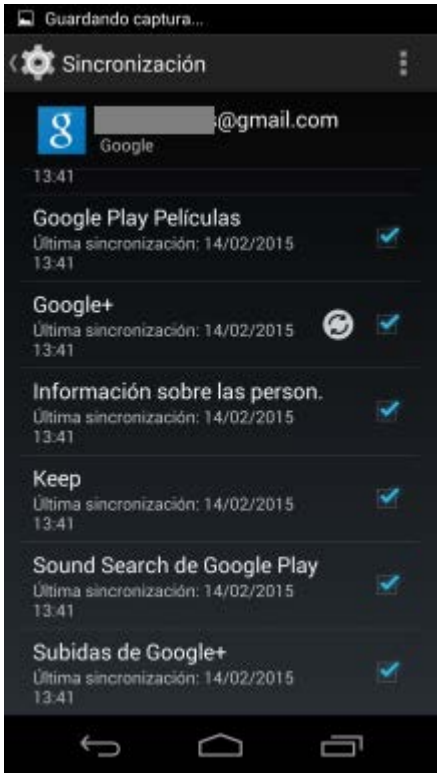


1021. A través del botón de menú superior es posible forzar la sincronización de la cuenta mediante la opción "Sincronizar Ahora":



1022. Seleccionando una cuenta de usuario de Google concreta desde el menú " Ajustes - [Cuentas] - Google [Cuentas]" se permite el acceso a todas sus opciones generales de sincronización (descritas a continuación):





1023. Adicionalmente, desde el menú "Google [Privacidad]" es posible configurar las opciones de configuración relacionadas con tres aspectos: las búsquedas ("Búsqueda", correspondientes a Google Now, ver apartado "5.21. Google Now"), la ubicación ("Ubicación", correspondientes a los servicios de ubicación, ver apartado "5.10.1. Servicios de ubicación de Google"), y los anuncios ("Anuncios", correspondientes a la configuración de anuncios, ver apartado "5.18.2. Anuncios").

1024. Las opciones de sincronización de la cuenta de usuario de Google permiten establecer qué tipo de datos e información, y por tanto servicios, serán sincronizados entre el dispositivo móvil y Google, y en concreto, la cuenta de usuario vinculada al mismo (ver imágenes superiores).

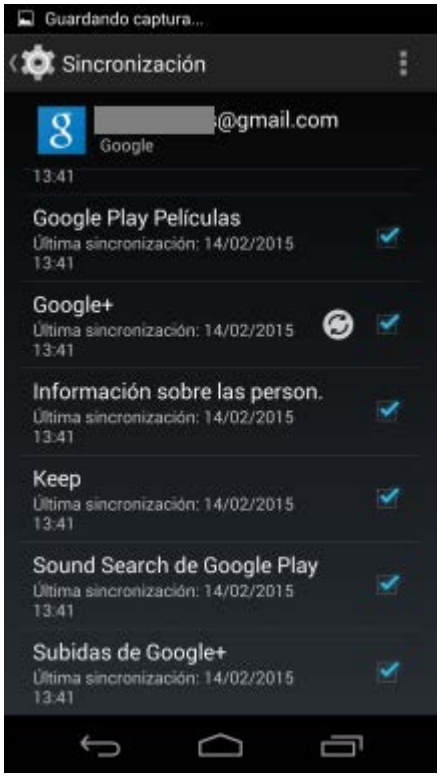
1025. Por defecto, todos los servicios y tipos de datos asociados están habilitados para su sincronización, y ésta se lleva a cabo de manera automática.

1026. Los servicios incluidos para su sincronización en Android 4.x incluyen el calendario, el navegador web Chrome, los contactos, los datos de las apps, Drive, Fotos (de Google+), Gmail, Fotos (de Google), Google Play (incluyendo los libros, el kiosco, la música, y las películas), Google+, información sobre las personas, Keep, búsquedas mediante audio en Google Play y las subidas de Google+.

1027. Desde el punto de vista de seguridad se recomienda deshabilitar todos y cada uno de los servicios de los que el usuario no esté haciendo uso y/o para los que no se desea hacer un uso explícito de la sincronización, simplemente, desmarcando la casilla correspondiente de la parte derecha.

1028. Al deshabilitar la sincronización de cada opción o servicio, los datos asociados no serán eliminados del dispositivo móvil. Los datos sólo pueden borrarse eliminando la cuenta.

1029. A través del botón de menú superior es posible forzar la sincronización de la cuenta con la opción "Sincronizar Ahora", o eliminar la misma, mediante la opción "Eliminar cuenta":



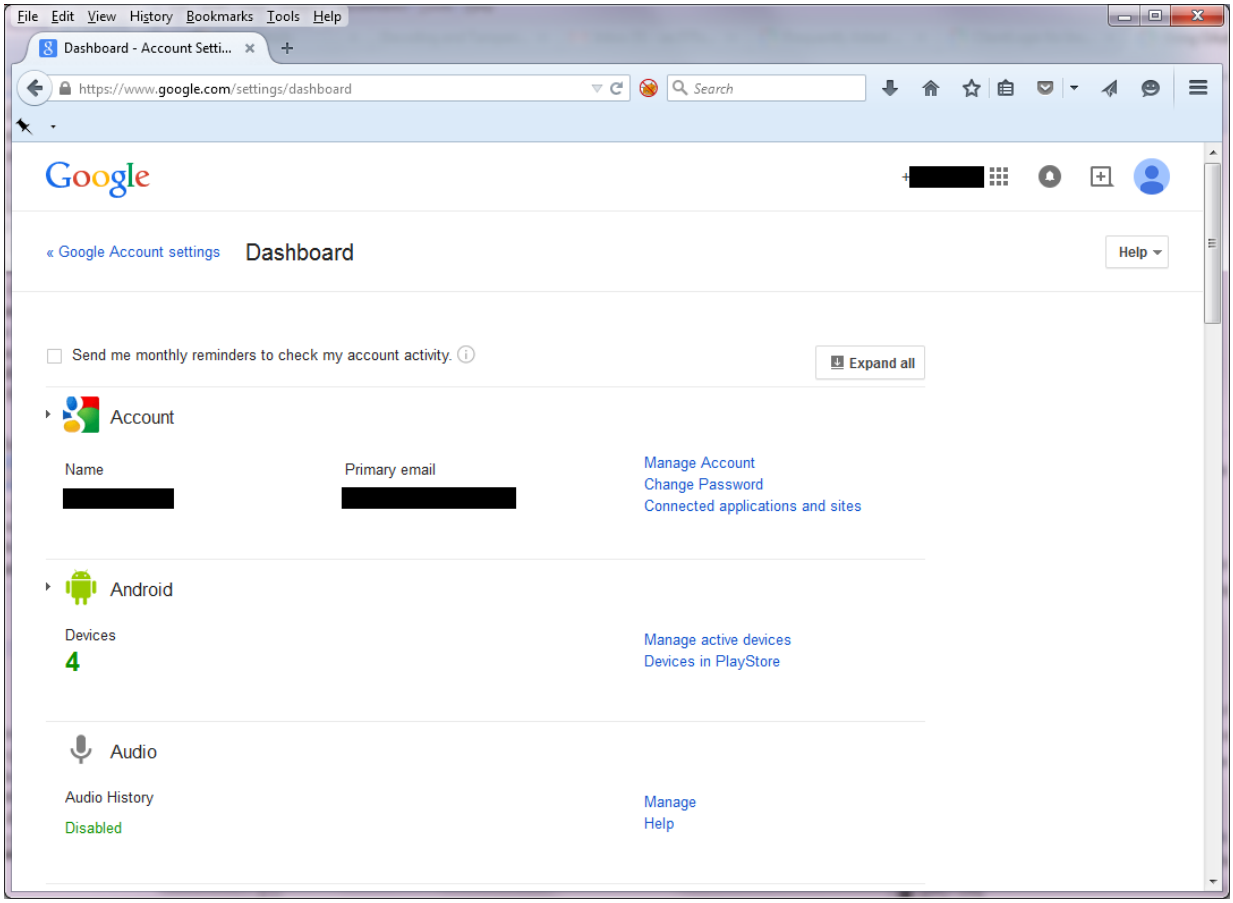
1030. La sincronización de la información de los diferentes servicios de Google en Android 4.x se realiza mediante conexiones HTTPS cifradas[96] [Ref.- 108].

1031. En el pasado (hasta abril de 2012), el protocolo de autentificación ClientLogin era empleado por las apps de Android que interactúan con los servicios y APIs de Google para obtener un *token* de autentificación (authToken), mediante el envío de las credenciales válidas (usuario y contraseña) de una cuenta de usuario de Google a través de HTTPS. El authToken, denominado "auth", era intercambiado a través de la cabecera "Authorization: GoogleLogin auth=…" de HTTP.

1032. El authToken era empleado para el acceso a las interfaces (o APIs) de los servicios de Google, de forma similar al uso de sesiones mediante cookies en aplicaciones web, y su valor era válido durante (como máximo) dos semanas (14 días) [Ref.- 110].

1033. En la actualidad, ClientLogin ha sido reemplazado por OAuth 2.0 [Ref.- 112], mecanismo de autentificación y autorización qué también permite a las apps de Android interactuar con los servicios y APIs de Google.

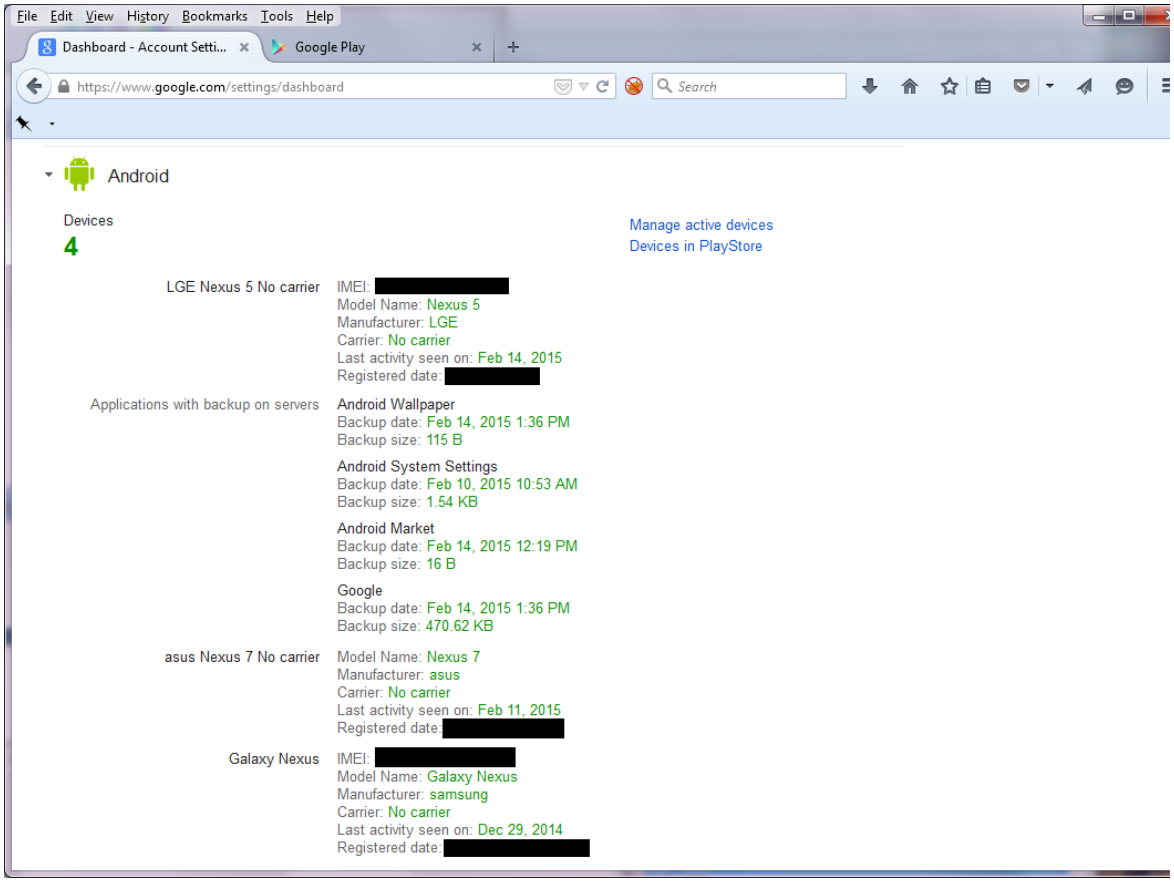
1034. Finalmente, en el caso de usuarios individuales no asociados a un dominio de Google Apps (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android") es posible acceder a la información de la cuenta a través del Panel de Control de Google (o *dashboard*), disponible en "https://www.google.com/dashboard/":



1035. Dentro de las opciones disponibles se encuentra la gestión de la cuenta de usuario de Google, de los dispositivos móviles vinculados, de todos los servicios de Google (Audio,

[96] En versiones previas de Android, 2.x, algunos servicios de Google empleaban tráfico HTTP sin cifrar.

Calendario, sincronización de Chrome, Cloud Print, Contactos, Gmail, Google Fotos, Google+, histórico de ubicaciones, Play Store o Google Play, perfil, histórico de búsquedas, Talk, y YouTube), siendo posible acceder a todos los detalles de cada servicio, como por ejemplo, gestionar las apps instaladas desde Google Play (a través de un enlace directo a la cuenta de usuario de Google en Google Play: "https://play.google.com/store/account?hl=es/"), así como verificar los datos almacenados por Google para los dispositivos móviles vinculados a la cuenta. Estos datos incluyen, entre otros, para cada dispositivo móvil su IMEI, modelo, fabricante, operador de telefonía, fecha de registro, fecha de la última actividad, etc., así como una lista de las apps que almacenan una copia de seguridad de sus datos en los servidores de Google:

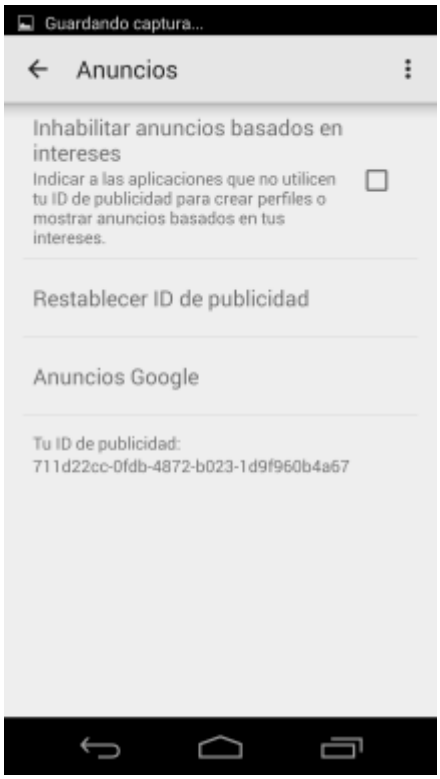


5.18.2 ANUNCIOS

1036. La configuración de anuncios está asociada a la cuenta de usuario de Google (ver apartado "5.18.1. Asignación de una cuenta de usuario de Google al dispositivo móvil"), y también está disponible a través de la opción "Anuncios" desde la app de "Ajustes de Google".

1037. En el caso de la configuración de anuncios, el usuario puede "Inhabilitar anuncios basados en intereses", seleccionando dicha opción (no habilitada por defecto), acción recomendada desde el punto de vista de la privacidad para indicar que las apps no usen el ID de publicidad del usuario para mostrar anuncios en base a sus intereses. Esta opción hará que los anuncios mostrados sean más genéricos, y aunque muy probablemente no serán del interés del usuario, evita que se haga un seguimiento del usuario en este tipo de servicios:

1038. Por otro lado, el usuario en cualquier momento puede restablecer el identificador de publicidad, mediante la opción que lleva este mismo nombre. El ID (o identificador) de publicidad es un número aleatorio y único (supuestamente anónimo) que se genera en el momento de la instalación inicial del dispositivo móvil, o cada vez que es restablecido, y se emplea por los servicios de anuncios, asociados a Google Play y las apps de terceros, para hacer un seguimiento del usuario [Ref.- 183]:



1039. El ID de publicidad está visible en la parte inferior de esta pantalla, y al ser restablecido es posible confirmar cómo ha cambiado su valor.

1040. Desde agosto de 2014, y con el objetivo de proteger la privacidad del usuario, Google Play (y sus servicios de anuncios) obligó a todas las apps de terceros a hacer uso del ID de publicidad (funcionalidad disponible desde octubre de 2013 mediante la versión 4.0 de los servicios y app de Google Play) para llevar a cabo cualquier tarea de seguimiento del usuario con fines publicitarios, en lugar de emplear (tal cómo hacían numerosas apps en el pasado) otros identificadores persistentes vinculados al usuario o al dispositivo móvil, como por ejemplo el identificador de la cuenta de usuario de Google, el IMEI del terminal, el IMSI de la tarjeta SIM, etc [Ref.- 183].

1041. Se recomienda desde el punto de vista de la privacidad que el usuario periódicamente acceda a este menú y restablezca el valor de ID de publicidad, para evitar que se pueda realizar una correlación del usuario y sus hábitos y actividades a medio y largo plazo.

1042. Por último, la opción "Anuncios Google" redirige al usuario a la página web de Google relativa a los servicios de anuncios y publicidad.

5.18.3 GESTIÓN DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO DE GOOGLE

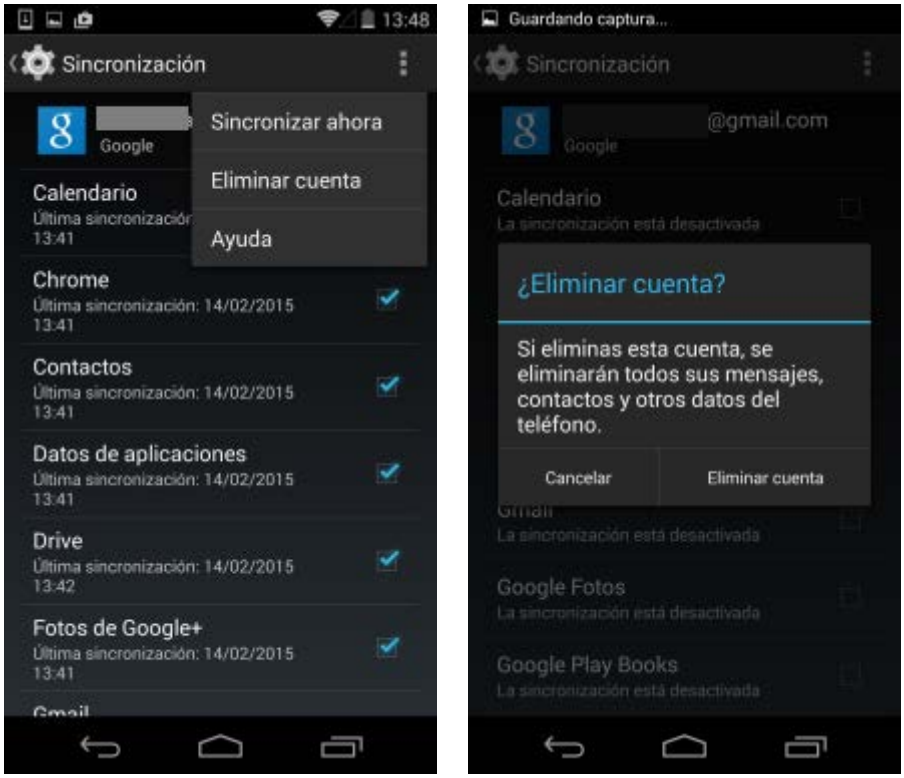
1043. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña de la cuenta del usuario de Google en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a la cuenta del usuario, junto a todos sus servicios asociados, como por ejemplo Google Play.

1044. Sin embargo, no se ha identificado ninguna opción de configuración en el dispositivo móvil, a través de "Ajustes [Cuentas]" o "Ajustes [Personal] - Seguridad" (o en la configuración de la app "Play Store"), para evitar el almacenamiento de la contraseña (o de los *tokens* de autentificación) de la cuenta de usuario de Google.

1045. Es decir, la contraseña (o *token* de autentificación) asociada a la cuenta del usuario queda almacenada automáticamente en el dispositivo móvil, no siendo posible evitar su almacenamiento. Como resultado, tras encender el dispositivo se dispone de acceso directo y completo a la cuenta del usuario y a todos los servicios asociados.

1046. Este escenario de gestión y almacenamiento automático de contraseñas para las cuentas del usuario es similar para las cuentas de otros servicios, por ejemplo redes sociales como Facebook o Twitter, dónde la contraseña queda almacenada en la app y, por tanto, en el dispositivo no siendo posible evitar que no sea así.

1047. La alternativa principal identificada para evitar esta asociación entre cuenta/contraseña y dispositivo móvil es únicamente eliminar la cuenta asociada. La pantalla de detalles de una cuenta permite eliminarla del dispositivo móvil mediante el botón "Eliminar cuenta":



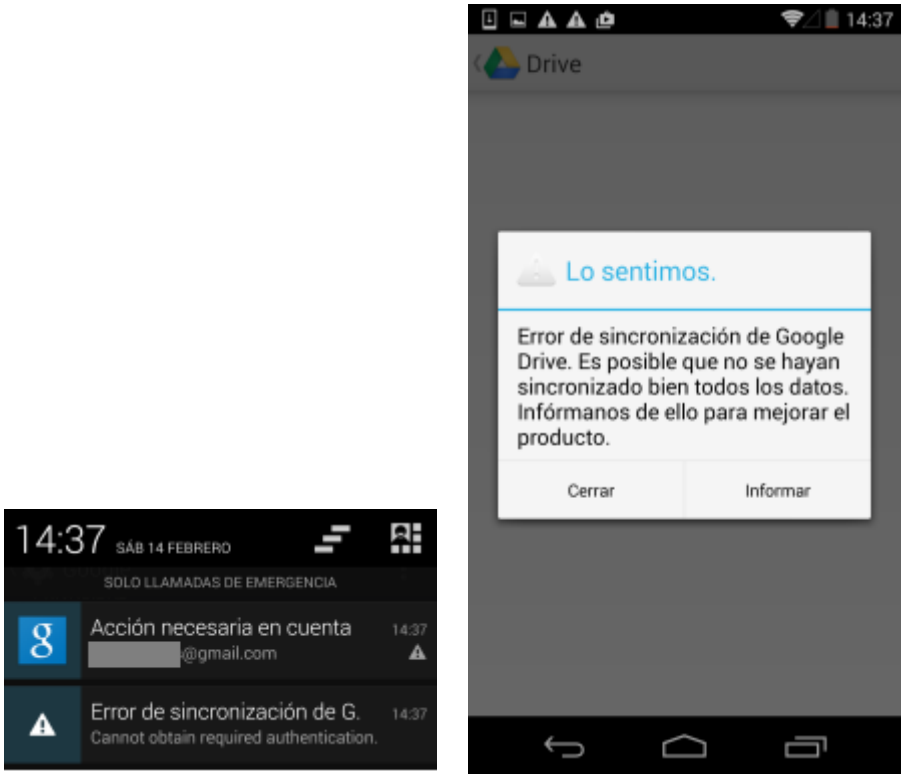
1048. Android no proporciona capacidades para modificar la contraseña de la cuenta principal de Google asociada al dispositivo móvil, ni para modificar las contraseñas de otros servicios disponibles en Android.

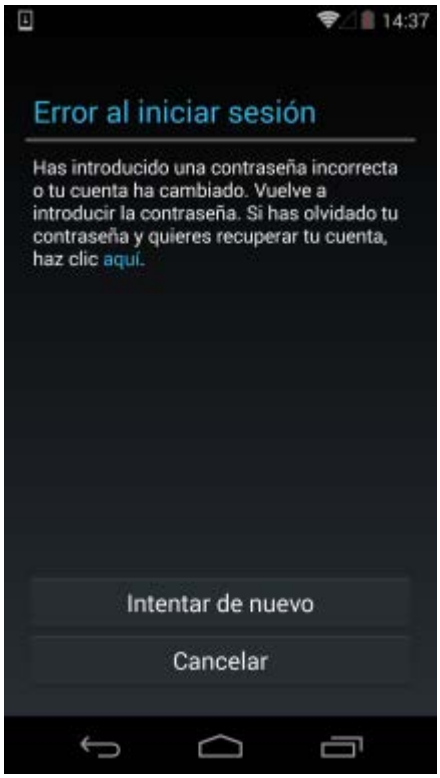
1049. Las siguientes recomendaciones aplican tanto a la cuenta principal de Google como a las cuentas de otros servicios, como Twitter o Facebook. Para otros servicios será necesario evaluarlo independientemente, y en todo caso, hacer uso del acceso web estándar a los mismos.

1050. Para invalidar la contraseña almacenada para la cuenta principal de Google asociada al dispositivo móvil, el método más directo pasa por modificar la contraseña a través de la página web estándar del servicio, desde otro ordenador o desde el propio navegador web del dispositivo móvil Android.

1051. Tras acceder a Google (Google Accounts: https://www.google.com/accounts) y modificar la contraseña de la cuenta, la próxima vez que se acceda desde el dispositivo móvil a alguna de las apps que hacen uso de los servicios de Google (por ejemplo, Gmail, Google Play, Google Drive, etc), y por tanto, de dicha cuenta, Android generará una notificación de error de sincronización (visible también desde la barra superior de estado) y solicitará al usuario la (nueva) contraseña para la cuenta[97]:

[97] Algunas apps o servicios concretos de Google también pueden generar sus notificaciones, como Google Drive.





Nota: la solicitud de la contraseña asociada a la cuenta del usuario también se puede presentar al cambiar la tarjeta SIM del dispositivo móvil, según la versión de Android y el modelo de terminal empleado.

1052. En caso de sustracción o pérdida del dispositivo móvil, este cambio de contraseña a través de la web debería ser una de las primeras tareas a realizar por el usuario.

1053. Por otro lado, debido a que Android está diseñado para trabajar con una cuenta de usuario de Google que esté siempre activa, tampoco proporciona capacidades para desconectarse (o cerrar la sesión actual) de la cuenta de usuario de Google, de forma que la próxima vez que se utilice cualquiera de los servicios asociados, y se establezca una sesión con estos, se solicite de nuevo al usuario la contraseña de la cuenta.

1054. El método disponible para forzar esta desconexión, sin tener que eliminar la cuenta del dispositivo móvil y/o resetear el mismo, pasa por cambiar la contraseña desde la web (como se ha descrito previamente) o utilizar apps de terceros con este propósito.

1055. En versiones previas de Android, 1.x, era posible forzar esta desconexión borrando la caché y los datos asociados a algunos de los servicios críticos de conexión y sincronización con Google (Gmail, Google Apps y Gmail Storage). Los botones "Borrar datos" y "Borrar caché" estaban disponibles a través del menú de "Ajustes - Aplicaciones - Administrar aplicaciones", desde la pestaña "Todas", seleccionando una por una estas aplicaciones (o servicios). Esta recomendación no aplica desde Android 2.x.

5.19 AUTENTIFICACIÓN DE DOS FACTORES EN LA CUENTA DE USUARIO DE GOOGLE

1056. El acceso a la cuenta de usuario de Google, ya se trate de un usuario particular o individual, o de un usuario perteneciente a una organización o dominio asociado a Google Apps (aplicaciones de Google), puede ser protegido por un mecanismo de verificación en dos pasos más seguro que la utilización de sólo un usuario y su contraseña asociada [Ref.- 15].

1057. En lugar de emplearse únicamente las credenciales estándar de acceso del usuario a la cuenta de usuario de Google, basadas en un nombre de usuario y una contraseña, la verificación en dos pasos (*two-step verification*, o autentificación de dos factores) requiere que el usuario introduzca adicionalmente a su contraseña (algo que conoce) un código obtenido mediante su dispositivo móvil (algo que posee).

1058. El código de acceso o verificación puede ser obtenido en el dispositivo móvil a través de la app Google Authenticator [Ref.- 14], disponible en Google Play y que no requiere de conexión a Internet o a ninguna otra red de comunicaciones (servicio de telefonía móvil o de datos) para la generación de los códigos de verificación, o mediante un mensaje de texto (SMS) o una llamada de teléfono (requiriendo ambos disponer de servicio de telefonía).

1059. Adicionalmente, para disponer de un nivel de seguridad adicional en la cuenta de usuario de Google, en lugar de utilizar códigos de verificación, es posible utilizar una llave de seguridad[98] (compatible con el estándar abierto "FIDO Universal 2nd Factor (U2F)") que debe ser insertada en un puerto USB del ordenador, y hacer uso del navegador web Google Chrome, versión 38 o superior (esta opción de autentificación no está disponible para dispositivos móviles Android).

1060. En el caso de que el usuario no disponga del dispositivo móvil para obtener el código de verificación, es posible usar un número de teléfono alternativo (para recibir el código de verificación vía SMS o llamada telefónica), o también existe la posibilidad de imprimir o descargar códigos alternativos de un sólo uso, por ejemplo, para ser usados cuando el usuario se encuentra en el extranjero viajando.

[98] https://support.google.com/accounts/answer/6103523?hl=es

5.20 COPIAS DE SEGURIDAD

5.20.1 COPIA DE SEGURIDAD LOCAL

1061. Desde la versión 4.0 de Android (*Ice Cream Sandwich*) se dispone de capacidades locales para realizar copias de seguridad de los contenidos del dispositivo móvil en el ordenador del usuario [Ref.- 90], sin necesidad de haber realizado el proceso de *rooting* sobre el mismo.

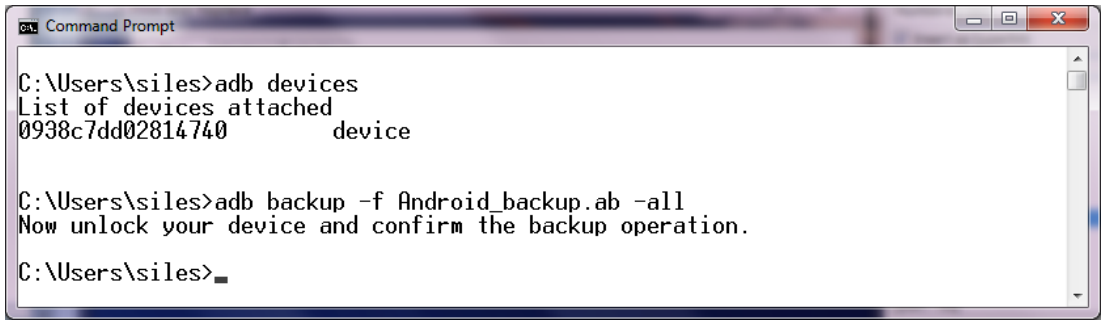
1062. Las copias de seguridad se llevan a cabo a través de ADB, por lo que es necesario disponer de las capacidades de desarrollo y depuración a través de USB habilitadas (ver apartado "5.11.3. Opciones de desarrollo y depuración USB").

1063. Desde el punto de vista de seguridad se recomienda habilitar estas capacidades únicamente en el momento de llevar a cabo la copia de seguridad, y volverlas a deshabilitar inmediatamente después.

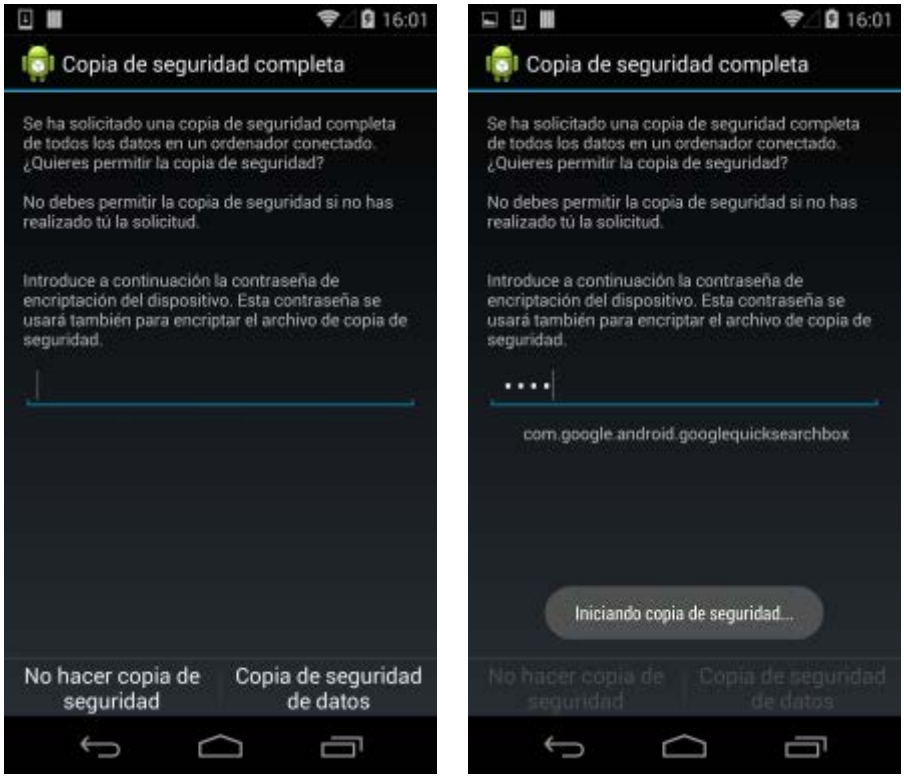
1064. En concreto, el comando "adb backup" permite realizar la copia de seguridad, pudiéndose especificar el fichero dónde se almacenará la misma (mediante la opción "-f", y por defecto en "backup.ab"). Este comando dispone de diferentes opciones para definir qué contenidos serán añadidos a la copia de seguridad, incluyendo los datos de las apps, tanto de sistema (o apps existentes por defecto) como de terceros, los propios ficheros APK de las apps, los contenidos del almacenamiento compartido (o tarjeta SD), etc. Es también posible especificar que se realice la copia de seguridad sólo de ciertas apps.

1065. Algunas apps pueden especificar en su fichero *manifest* que no permiten que se haga copia de seguridad de ellas, por lo que quedarán excluidas de este proceso.

1066. El fichero creado incluye una cabecera específica para las copias de seguridad de Android (variable según si se usa cifrado o no) y emplea el formato TAR [Ref.- 90].



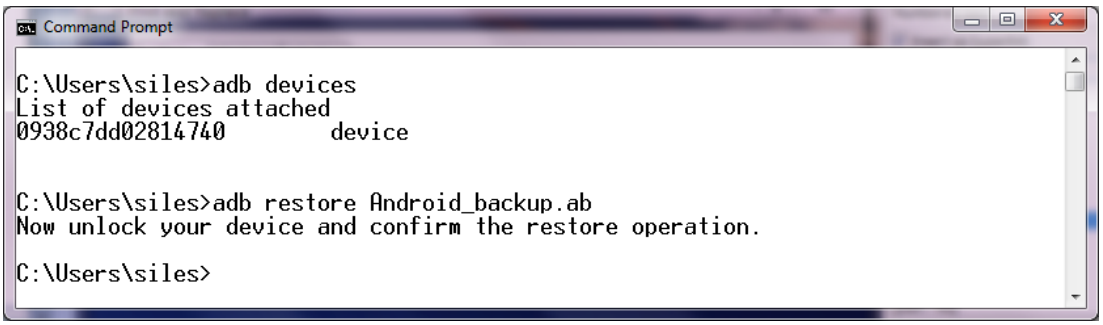
1067. Tras ejecutar el comando "adb backup", el dispositivo móvil mostrará una pantalla de confirmación para autorizar la realización de la copia de seguridad:



1068. Cabe destacar especialmente la opción qué permite establecer una contraseña para cifrar los contenidos de la copia de seguridad mediante AES 256 bits. Se recomienda siempre hacer uso de una contraseña para cifrar los contenidos de la copia de seguridad.

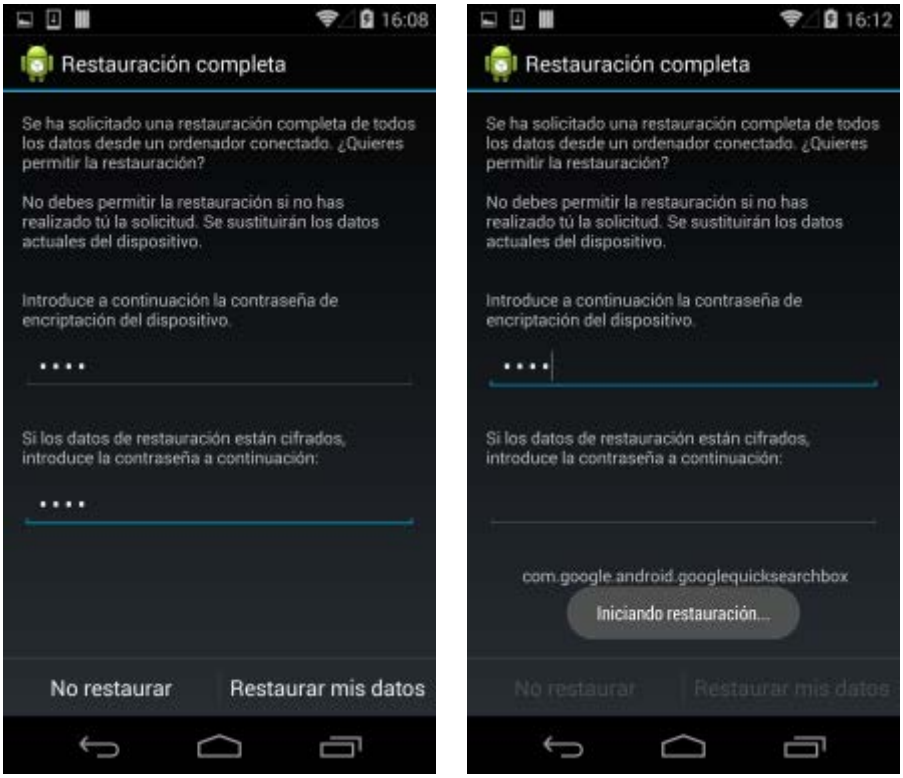
1069. Si el dispositivo móvil está cifrado, es obligatorio especificar el código de acceso como el valor de la contraseña empleada para la copia de seguridad, no siendo posible elegir una contraseña diferente y potencialmente más robusta qué, por ejemplo, un PIN de 4 dígitos.

1070. El comando equivalente "adb restore" permite recuperar o restaurar una copia de seguridad realizada previamente en el dispositivo móvil:



1071. En el caso de que la copia de seguridad esté cifrada, el proceso muestra en la pantalla del dispositivo móvil el campo para especificar la contraseña utilizada a la hora de realizar la copia de seguridad.

1072. En el caso en el que el dispositivo móvil está cifrado, es necesario especificar únicamente el código de acceso empleado para el cifrado (aunque ambos campos están habilitados):



5.20.2 COPIA DE SEGURIDAD EN LOS SERVIDORES DE GOOGLE

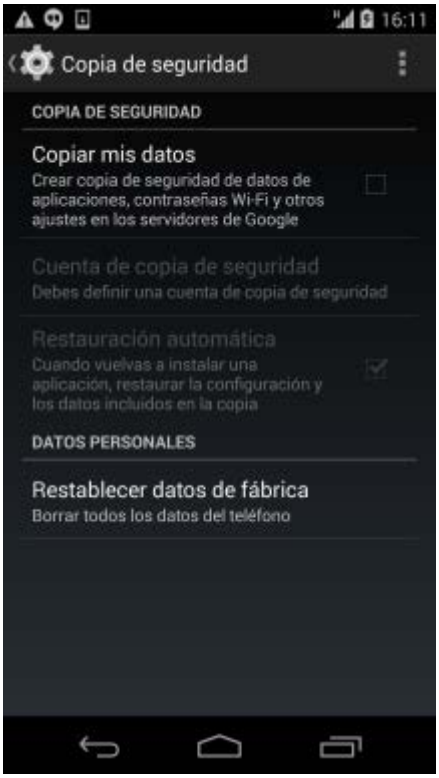
1073. El servicio de copia de seguridad de datos de Google (denominado *Android Backup Service*) permite almacenar información personal y datos del usuario en los servidores de Google, como los favoritos de navegación web, palabras añadidas al diccionario, una lista de las apps instaladas, parámetros de configuración y los datos utilizados por las apps de terceros, contraseñas de las redes Wi-Fi, la mayoría de parámetros de configuración del dispositivo móvil y de los servicios de Google, siendo posible restaurar los datos si fuese necesario reemplazar el dispositivo móvil o reinstalar una app [Ref.- 101].

1074. Durante el proceso de instalación y configuración inicial de Android y vinculación del dispositivo móvil (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial") a una cuenta de usuario de Google (y/o de creación de la cuenta) se solicita confirmación por parte del usuario para activar el servicio de copia de seguridad de datos (ver apartado "5.18. Cuenta de usuario de Google").

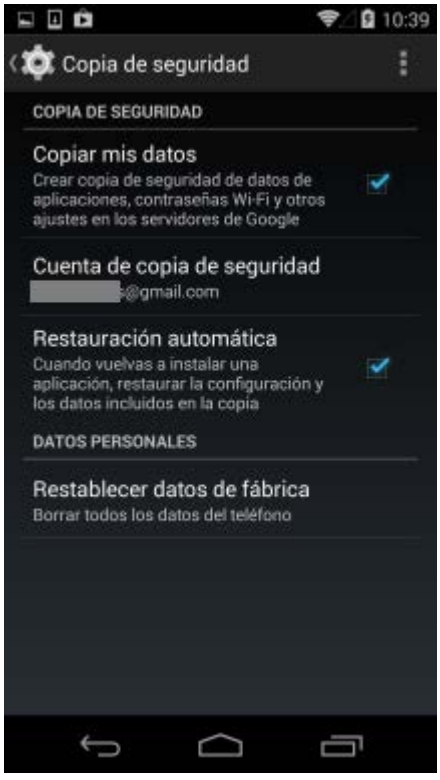
1075. En el caso de dispositivos móviles Android multiusuario, únicamente el usuario propietario (o usuario principal) puede gestionar las opciones de copia de seguridad y restauración.

1076. El servicio de copia de seguridad de datos en los servidores de Google puede ser activado o desactivado posteriormente a través del menú "Ajustes [Personal] - Copia de seguridad", y en concreto, mediante la opción "Copiar mis datos" (siendo necesario disponer de una cuenta de usuario de Google vinculada al dispositivo móvil).

1077. Al desactivar la opción, no se llevarán a cabo más copias de seguridad de los datos en la cuenta de usuario de Google asociada, y las copias de seguridad existentes serán (supuestamente) eliminadas de los servidores de Google.



1078. La opción "Cuenta de copia de seguridad" detalla la cuenta de usuario de Google vinculada al dispositivo móvil y en la que se están almacenando los datos. Es necesario disponer de al menos una cuenta, y es posible añadir cuentas de usuario de Google adicionales:



1079. Si se reinstala una app de terceros (desde Google Play), el servicio puede almacenar y restaurar la configuración y los datos asociados a la app (algunas apps pueden no permitir la realización de copias de seguridad y la restauración de sus datos).

1080. La opción "Restauración automática" permite restaurar la configuración y los datos asociados a una app al instalarla (o reinstalarla) en el dispositivo móvil desde la copia de seguridad disponible en Google. Si la app fue instalada y usada en el mismo, o en otro dispositivo móvil, en el que se disponía del servicio de copia de seguridad de datos activo con la misma cuenta de usuario de Google, toda la información de la app será recuperada.

1081. En caso de que el usuario reemplace, sustituya o renueve su dispositivo móvil, este servicio ofrece la posibilidad de restaurar los datos desde la copia de seguridad de Google en el nuevo dispositivo móvil la primera vez que se accede a Google con la cuenta de usuario asociada a este servicio.

1082. Los datos qué serán restaurados incluyen, entre otros, los ajustes de calendario y Gmail, los datos de redes Wi-Fi (incluyendo las credenciales y contraseñas de acceso), la configuración de la pantalla de inicio, los ajustes de idioma e introducción de texto, la lista de apps instaladas desde Google Play, junto a sus datos y ajustes de configuración, etc [Ref.- 101].

1083. El usuario u organización propietaria del dispositivo móvil Android debe evaluar el nivel de confianza depositado en Google para emplear este servicio y almacenar todos los datos personales y confidenciales del usuario.

5.20.3 COPIA DE SEGURIDAD DE FOTOS Y VÍDEOS

1084. El servicio de copia de seguridad de datos de Google (descrito en el apartado previo) no incluye las fotos (o fotografías) y vídeos disponibles en el dispositivo móvil.

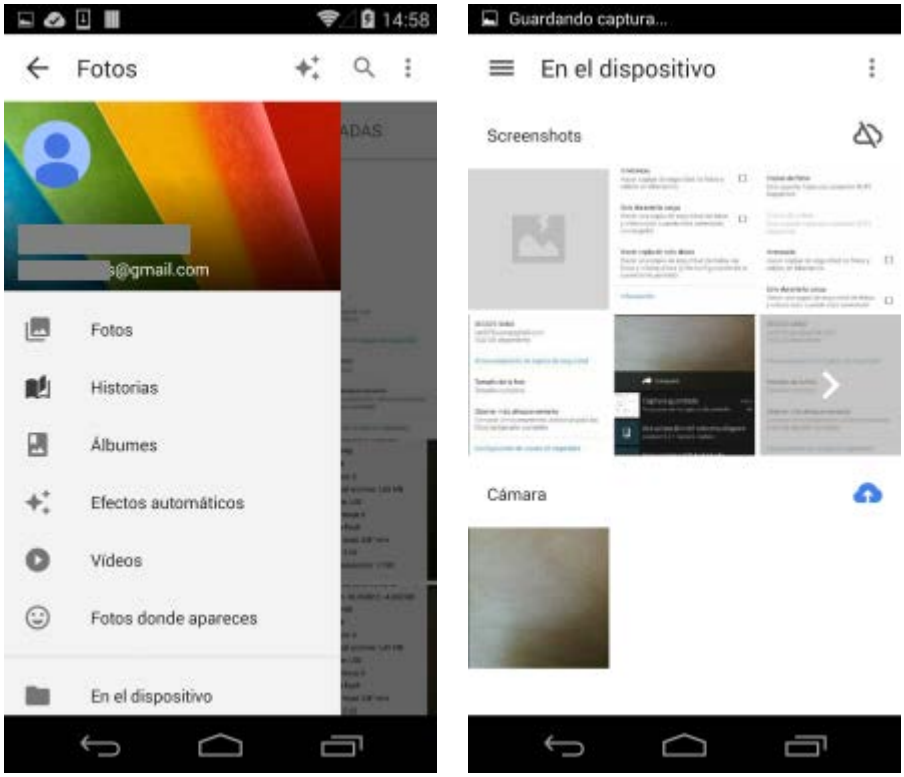
1085. Para hacer una copia de seguridad de las fotos y vídeos automáticamente en la cuenta de usuario de Google+ es necesario configurar el servicio de copia de seguridad de fotos y vídeos de Google (o específicamente, de Google+), disponible a través de la app "Fotos" [Ref.- 174]. Al activar este servicio, la copia de seguridad de las fotos y vídeos es (supuestamente) privada, salvo que el usuario decida compartirlas.

1086. Las fotos (y vídeos) incluyen tanto las realizadas con la cámara del terminal, como las capturas de pantalla (*screenshots*), las descargadas desde Internet y las que almacenan otras apps, como por ejemplo Hangouts.

1087. La primera vez que se ejecuta la app "Fotos" se consulta al usuario si quiere hacer copias de seguridad automáticamente de las fotos y vídeos, y si la transferencia de estos contenidos multimedia hacia la cuenta de usuario en Google se hará a través de redes Wi-Fi y redes de telefonía móvil (2/3/4G), con un posible gasto asociado, o sólo mediante redes Wi-Fi.

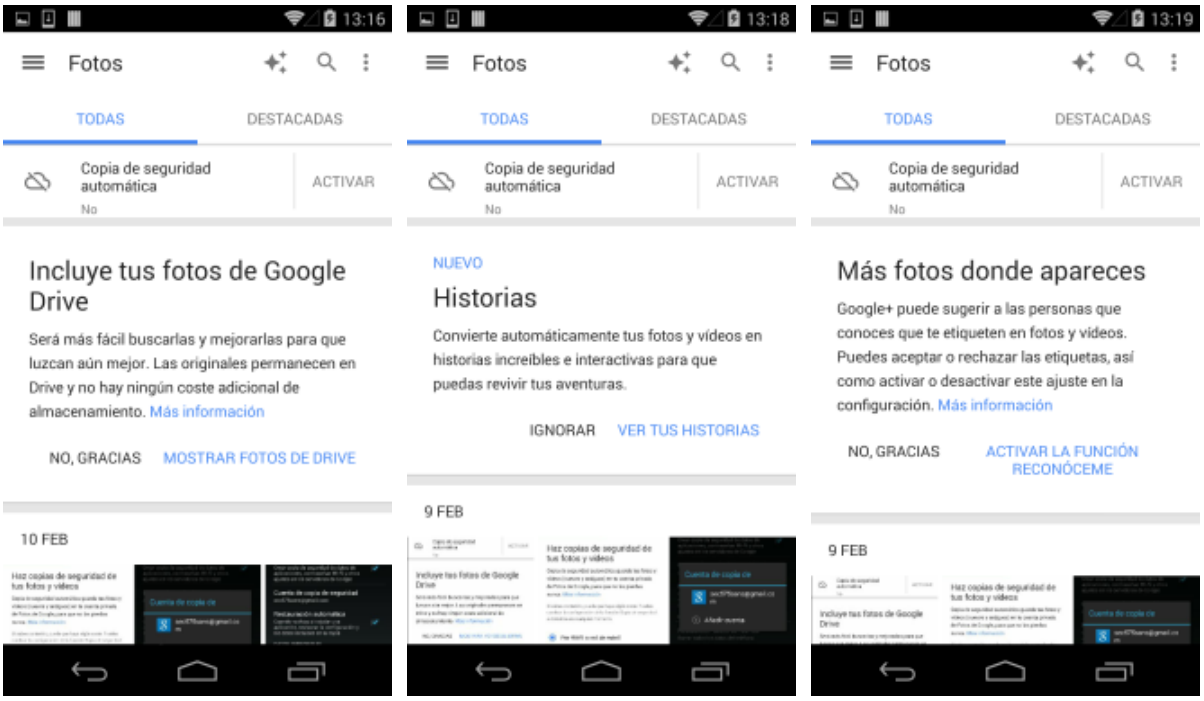
1088. La configuración inicial también permite añadir de manera general la copia de seguridad de las carpetas existentes en el dispositivo móvil, es decir, no sólo de las fotos y vídeos realizados con la cámara del terminal, sino también las correspondientes a las capturas de pantalla (*screenshots*), las descargadas desde Internet y las que almacenan otras apps.

1089. Es posible activar o desactivar las copias para carpetas concretas mediante la app "Fotos", el botón de menú superior izquierdo, y la opción "En el dispositivo" (en lugar de "Fotos"), seleccionando el icono de nube disponible a la derecha de cada carpeta [Ref.-174]:



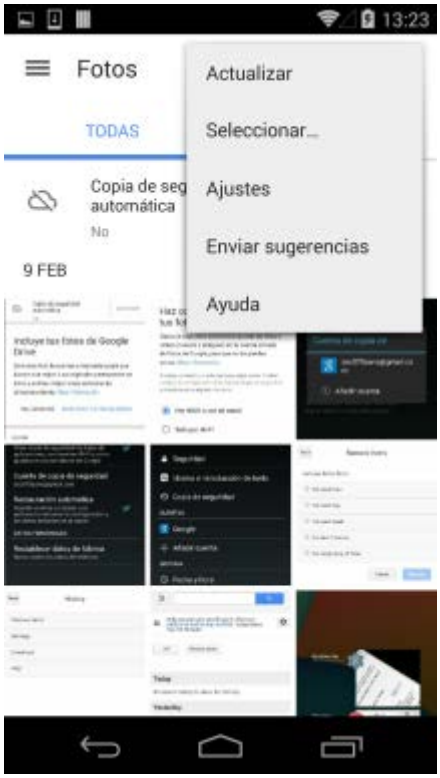
1090. Adicionalmente, en la configuración inicial se proporciona la opción al usuario de incluir en la copia de seguridad las fotos disponibles en su cuenta de usuario de Google Drive, de convertir las fotos y vídeos en historias (con un contexto geográfico asociado a

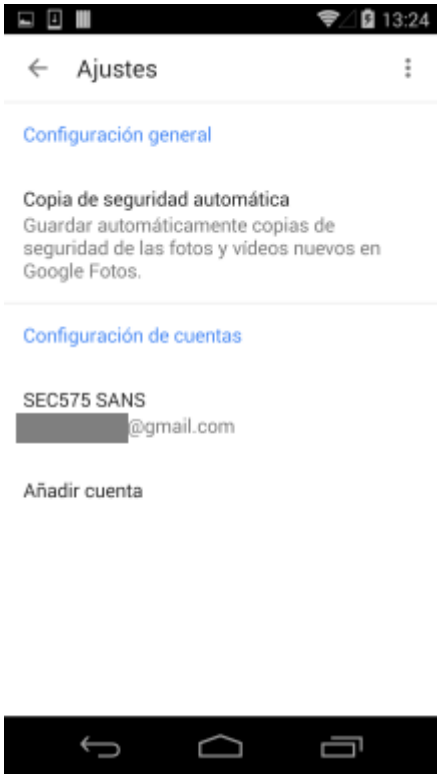
una visita o viaje, según su ubicación), y de activar la función de reconocimiento del usuario, sugiriendo a otros usuarios de Google+ el etiquetar fotos con la presencia del usuario:



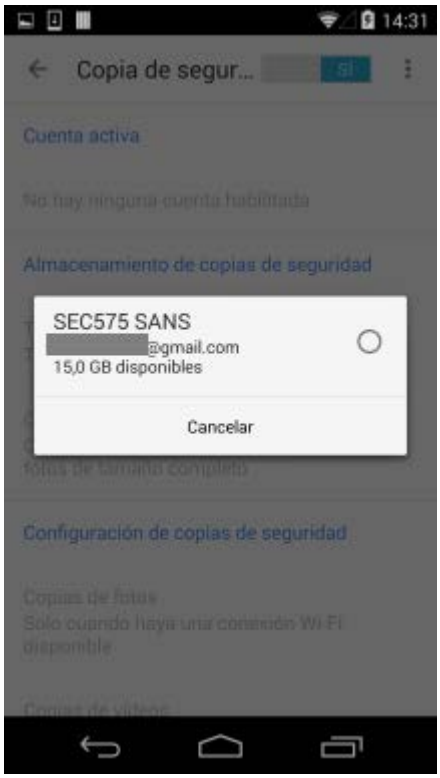
1091. Desde el punto de vista de seguridad se recomienda tener un control estricto de la copia de fotos y vídeos entre los diferentes servicios de Google y no habilitar estas capacidades, salvo que se quiera hacer un uso explícito de las mismas. Se dispone de opciones de configuración (descritas a continuación) para controlar estas funcionalidades.

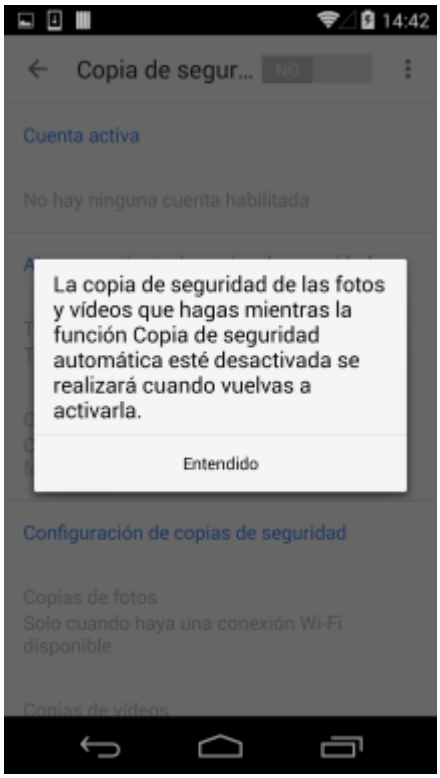
1092. Posteriormente, desde el icono de menú, a través de "Ajustes [Configuración general] - Copia de seguridad automática" es posible habilitar o deshabilitar esta funcionalidad mediante el botón "[SI | NO]":





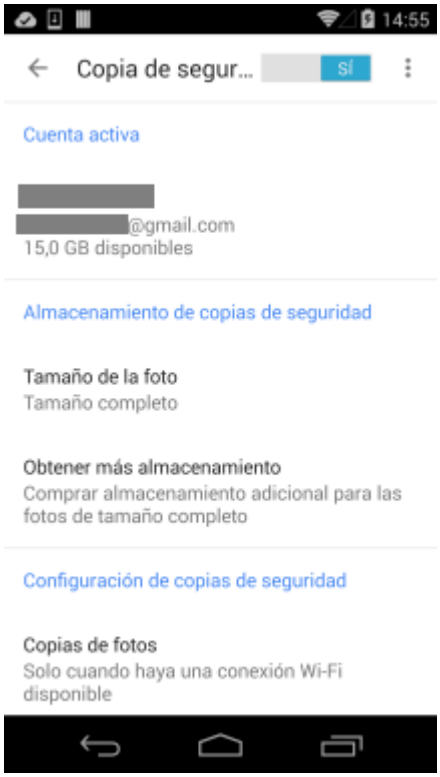
1093. Si se deshabilita la funcionalidad una vez ha sido habilitada, se muestra un mensaje que indica que la copia de seguridad de las fotos y vídeos que se realicen con la funcionalidad deshabilitada se llevará a cabo al volver a activarla posteriormente:



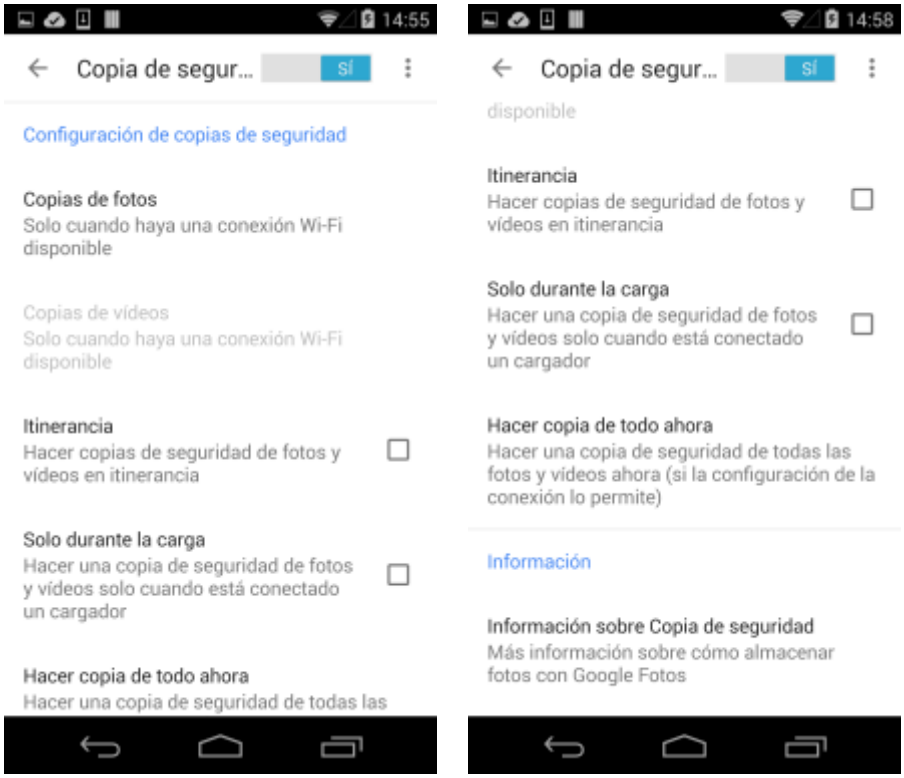


1094. Al activar la funcionalidad es posible acceder a los ajustes de configuración avanzados, disponiendo de información de la cuenta de usuario de Google asociada, del espacio disponible (15 GB por defecto en el momento de elaboración de la presente guía), y detalles del "Almacenamiento de copias de seguridad", como el tamaño por defecto de las

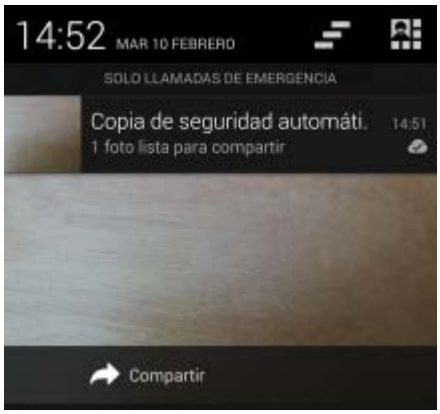
fotos (completo o estándar), la posibilidad de adquirir más almacenamiento con un coste asociado:



1095. La sección "Configuración de copias de seguridad" permite establecer los ajustes del tipo de redes a emplear para realizar las copias de fotos y vídeos por separado (mencionadas inicialmente), si se desea hacer uso de la funcionalidad en itinerancia (redes móviles en el extranjero), si la copia de seguridad sólo se llevará a cabo cuando el dispositivo móvil está cargando (y no al hacer uso de la batería únicamente), o forzar la realización de una copia de seguridad en el momento actual:



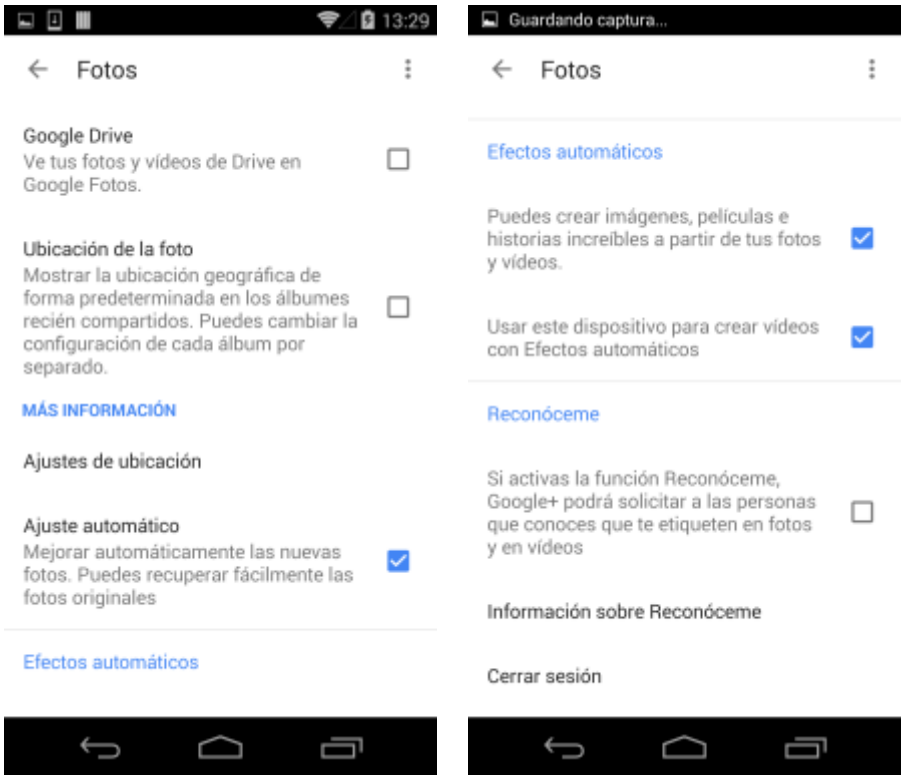
1096. Adicionalmente, al activar la funcionalidad se recibe una notificación que confirma que hay fotos disponibles en la copia de seguridad y que insta al usuario a compartirlas a través de Google+:



1097. La opción "Configuración de cuentas" dentro de "Ajustes" detalla la cuenta de usuario de Google vinculada al dispositivo móvil y en la que se están almacenando las fotos y vídeos. Es necesario disponer de al menos una cuenta, y es posible añadir y gestionar cuentas de usuario de Google adicionales.

1098. Si se selecciona la cuenta de usuario de Google, es posible configurar si estarán disponibles en Google Fotos las fotos y vídeos de Google Drive, y si se incluirá la ubicación geográfica de las fotos en los álbumes compartidos, pudiéndose cambiar esta configuración individualmente por cada álbum de fotos (opción "Ubicación de la foto"):

1099. Adicionalmente, los ajustes bajo "Más Información" permiten establecer los "Ajustes de ubicación" (ver apartado "5.10. Localización (o ubicación) geográfica"), y si las fotos serán mejoradas automáticamente, manteniendo una copia de las fotos originales (opción "Ajuste automático", habilitada por defecto). Asimismo, la sección "Efectos automáticos" permite crear historias a partir de fotos y vídeos (habilitada por defecto), y poder usar el dispositivo móvil para crear vídeos con efectos automáticos:



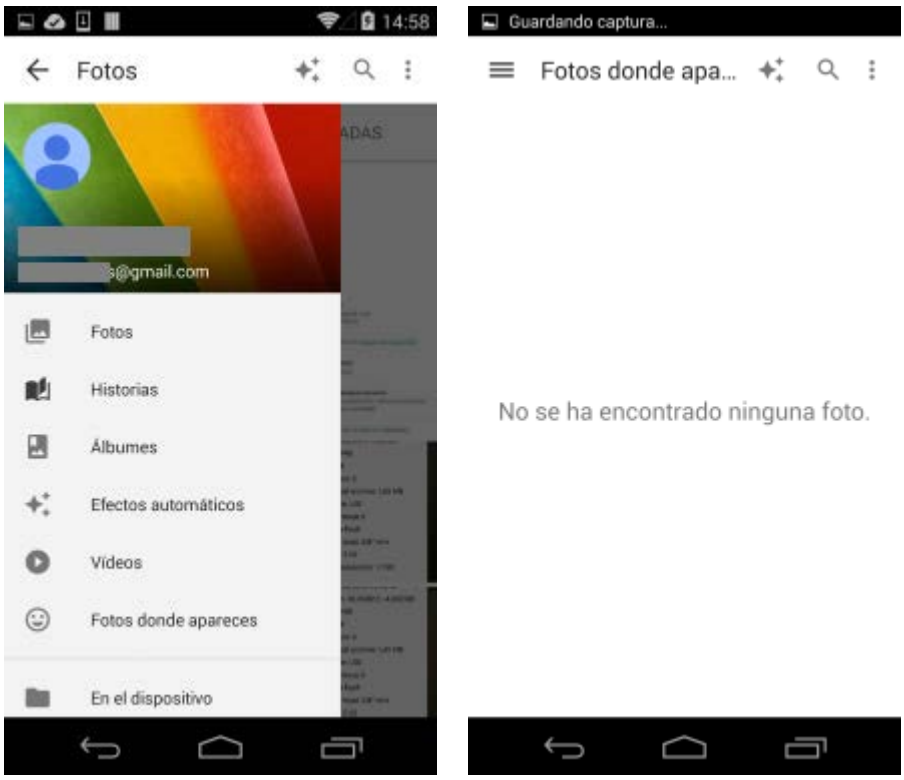
1100. Por último, la opción "Reconóceme" (deshabilitada por defecto) [Ref.- 175] permite a Google+ solicitar a otros usuarios que te etiqueten en fotos y vídeos, para que te puedan encontrar con más facilidad.

1101. Esta opción de configuración, junto a otras mencionadas previamente, también está disponible a través de la app "Google+`" y sus ajustes avanzados, debido a la estrecha integración entre Google+ y la app "Fotos".

1102. Al activar esta funcionalidad, Google+ crea un modelo de la cara del usuario en base a las fotos y vídeos en los que ya está etiquetado. Este modelo se actualiza con las nuevas fotos y vídeos recibidos, y puede ser eliminado desactivando esta opción en cualquier momento.

1103. En base a dicho modelo de cara, Google mostrará una sugerencia de etiqueta tanto al usuario como a sus conocidos cuando se identifique ese modelo o patrón de la cara del usuario en una nueva foto o vídeo. Si se desactiva esta opción, los conocidos del usuario dejarán de recibir sugerencias para etiquetar al usuario en las fotos o vídeos, sin embargo, las etiquetas ya añadidas no se eliminarán.

1104. La sección "Fotos donde apareces", disponible desde el menú superior izquierdo de la app "Fotos", permite aprobar o rechazar etiquetas (respondiendo a la pregunta "¿Eres tú?", así como revisar las fotos dónde el usuario ha sido etiquetado [Ref.- 176]:

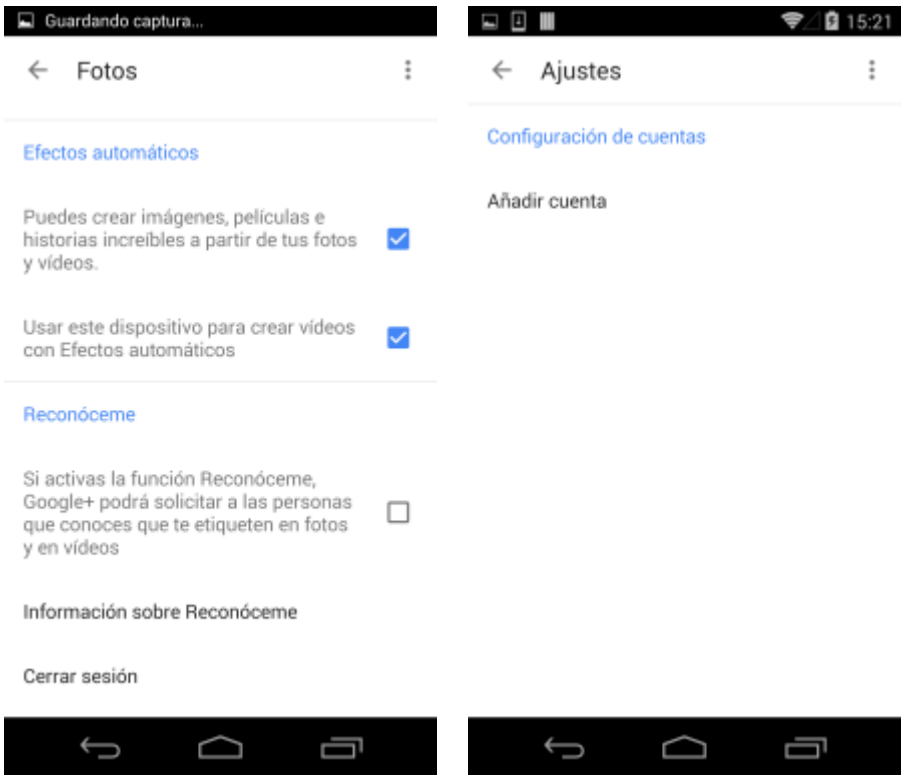


1105. Si se rechaza la etiqueta, ésta será eliminada de la foto. Una vez se aprueba una etiqueta, ésta se asociará al perfil de Google+ del usuario, y la foto aparecerá en la sección "Fotos donde apareces".

1106. Para eliminar una etiqueta, desde esta misma sección, es posible seleccionar la foto etiquetada y mediante el icono con una etiqueta en forma de cara de la parte inferior, emplear el icono de borrar (o papelera).

1107. Desde el punto de vista de seguridad, y de la privacidad del usuario, se recomienda no habilitar la funcionalidad de reconocimiento del usuario a través de fotografías y vídeos.

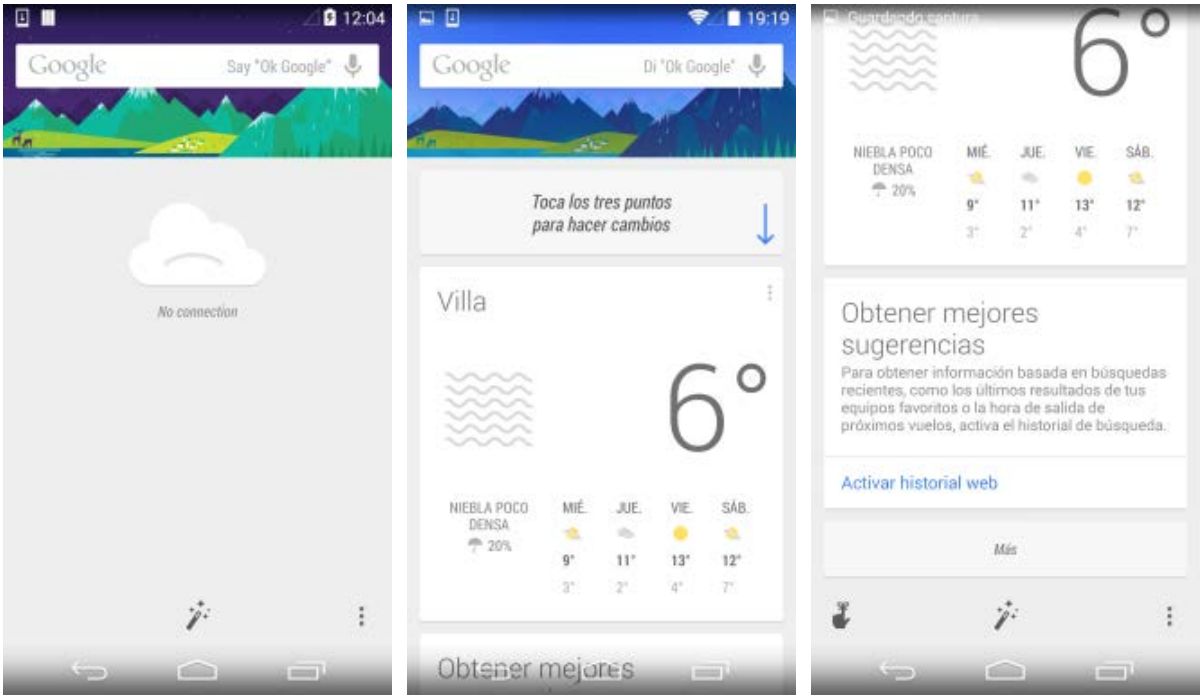
1108. Finalmente, la opción "Cerrar sesión" permite finalizar la sesión actual asociada a la cuenta de usuario de Google, incluida la vinculación entre éste y las fotos y vídeos del dispositivo móvil. Para poder hacer uso de la funcionalidad descrita es necesario volver a añadir una cuenta a través del botón de menú y la opción "Ajustes - Añadir cuenta":



5.21 GOOGLE NOW

1109. Google Now está siempre funcionando en segundo plano, analizando los datos de la actividad diaria del usuario, su ubicación (e histórico de ubicaciones) y mostrando las tarjetas de información (tarjetas Google Now o tarjetas Now) o notificaciones en función de los eventos que ocurren en tiempo real.

1110. Google Now proporciona su información principalmente a través de la app "Google", disponible para la realización de búsquedas a través de Google. La app "Google" está disponible desde una de las pantallas de inicio, desde el *Launcher*, o deslizando la pantalla desde la parte inferior hacia arriba, y permite ver las tarjetas de Google Now existentes, siempre que se disponga de conexión de datos (Wi-Fi o 2/3/4G):

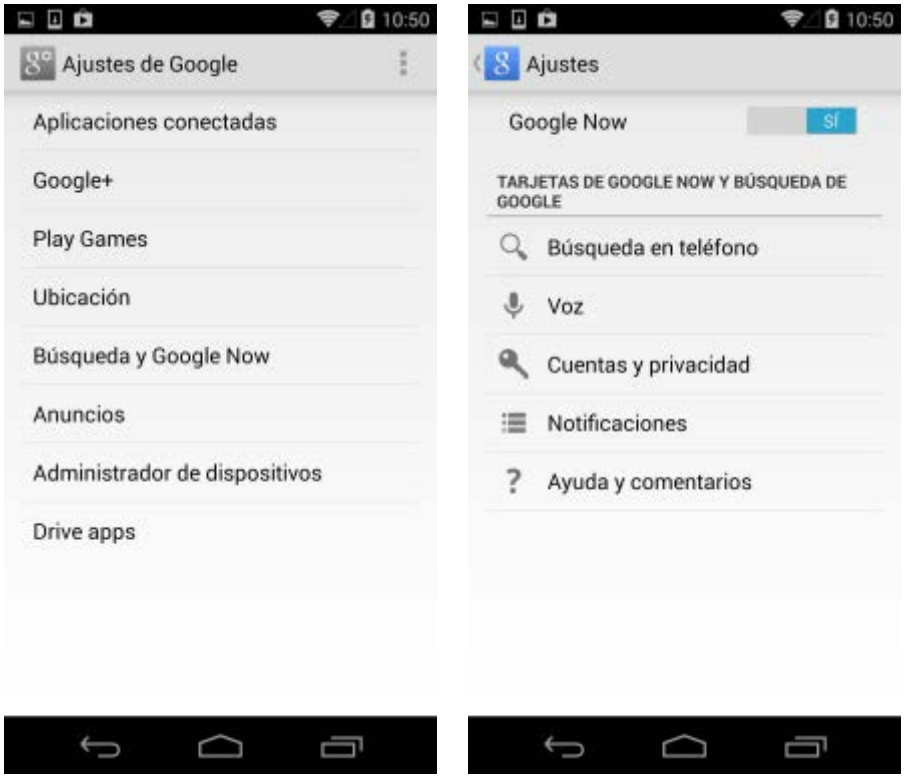


1111. La activación de Google Now se puede llevar a cabo durante el proceso de instalación y configuración inicial de Android (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial"), o posteriormente.

1112. Google Now hace uso de los servicios de ubicación (incluyendo el historial de ubicaciones; ver apartado "5.10.5. Historial de ubicaciones"), datos del calendario del usuario, sus búsquedas web (incluyendo el historial web; ver apartado "5.22.1.5. Historial de actividad web") y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros).

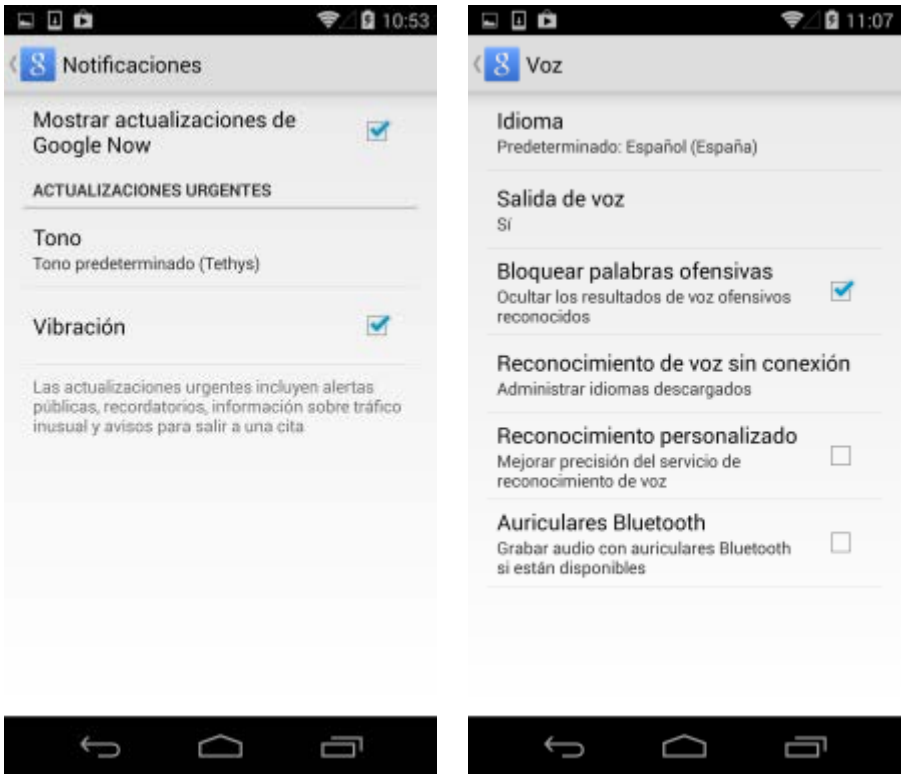
1113. Desde el punto de vista de seguridad y privacidad, salvo que se deseé hacer uso de la funcionalidad ofrecida por Google Now, debido a que conlleva un uso y análisis intensivo y muy elevado de los datos y actividades diarias del usuario, se recomienda no activar esta funcionalidad.

1114. Google Now puede ser desactivado en cualquier momento desde la app "Ajustes de Google" y el menú "Búsqueda y Google Now" y el botón "[SI | NO]" de Google Now. Adicionalmente, se dispone de diferentes opciones de configuración de la app Google bajo la sección "Tarjetas de Google Now y Búsquedas de Google":



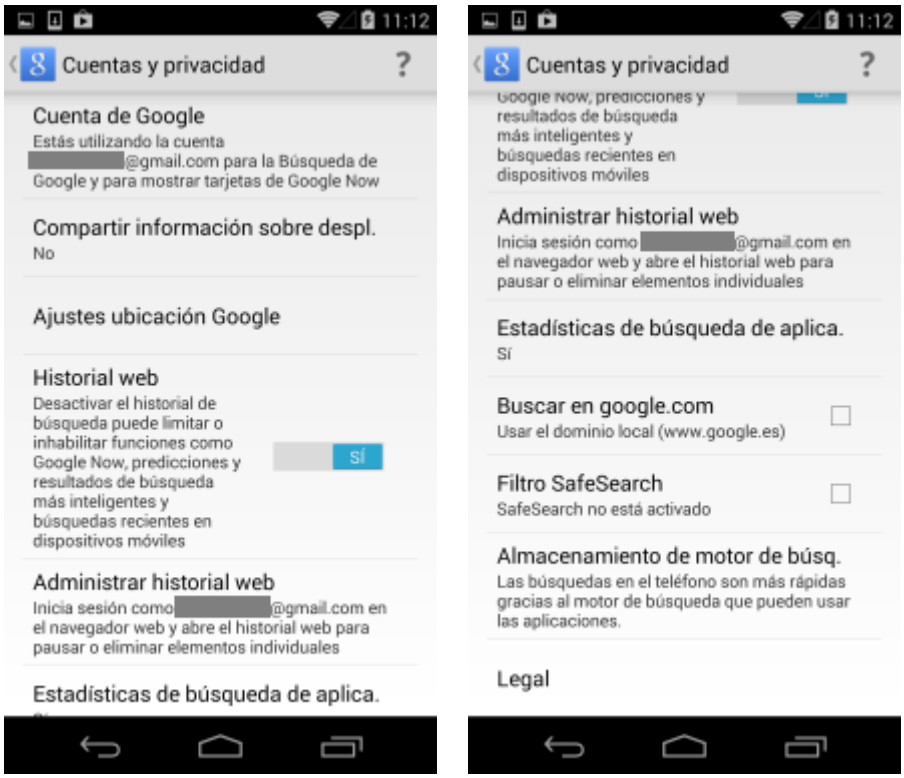
1115. Es posible también acceder a los ajustes de configuración desde la app "Google", el menú "..." de la parte inferior derecha, y la opción "Ajustes".

1116. Por ejemplo, es posible deshabilitar las tarjetas de información de Google Now desde el menú "Notificaciones" y la opción "Mostrar actualizaciones de Google Now":

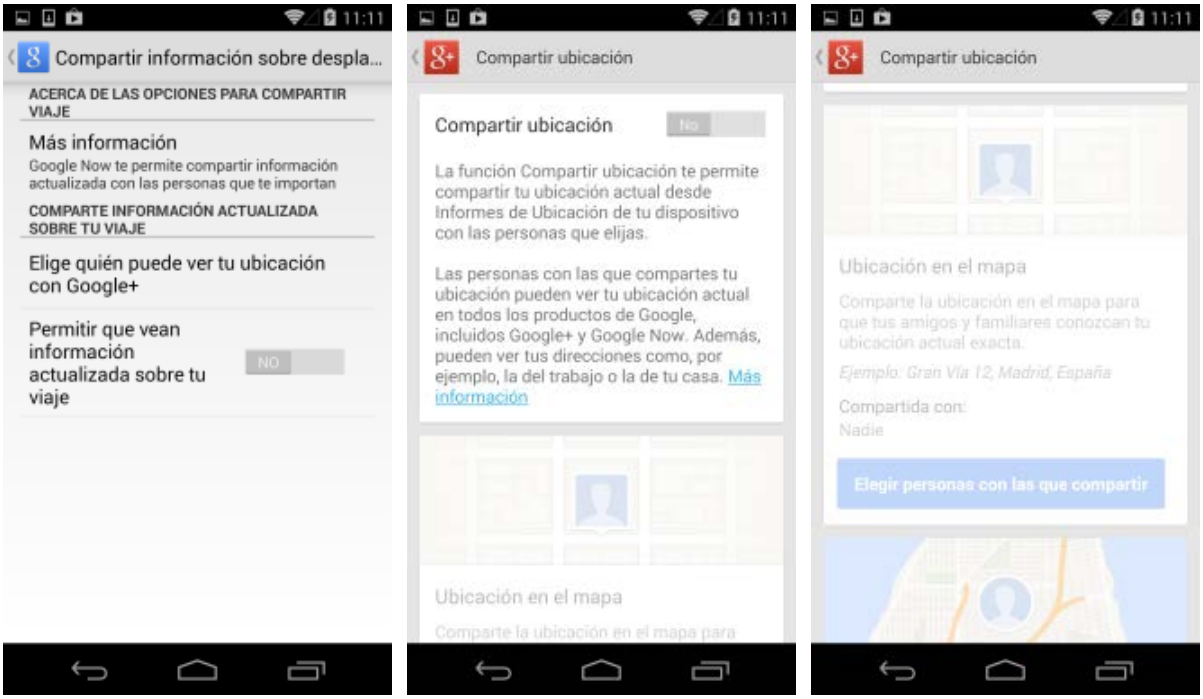


1117. El menú "Voz" permite configurar el idioma y otras capacidades asociadas a las búsquedas por voz (ver imagen superior derecha).

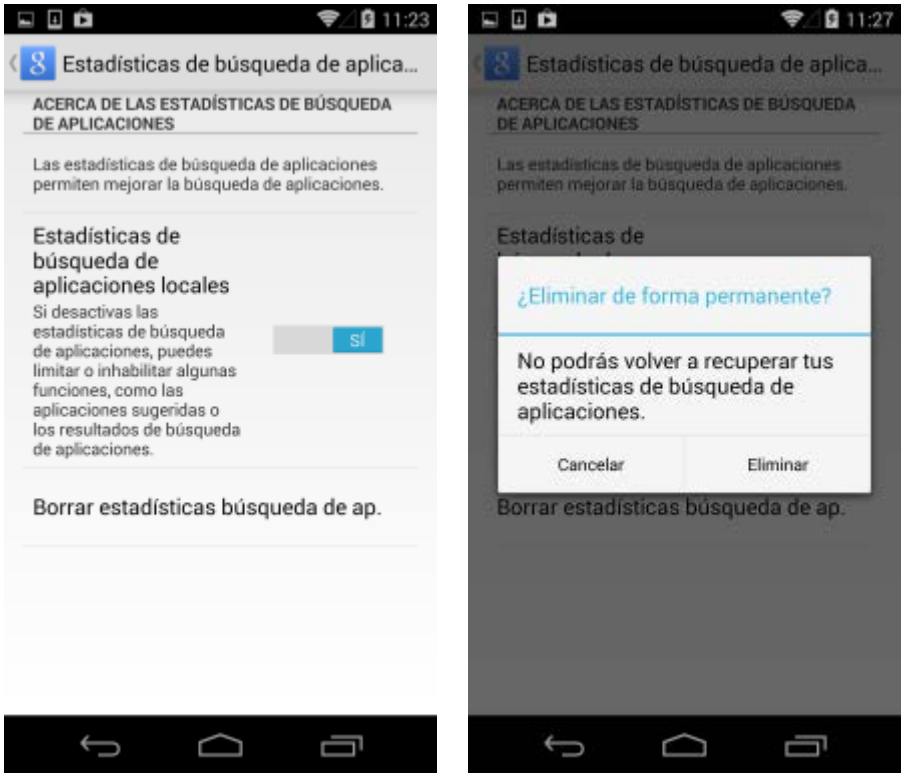
1118. El menú "Cuentas y privacidad" indica la cuenta de usuario de Google que se está empleando para las búsquedas en Google y para Google Now, la posibilidad de compartir información actualizada con otros usuarios sobre viajes y desplazamientos (funcionalidad deshabilitada por defecto), permite acceder a los ajustes de los servicios de ubicación (ver apartado "5.10. Localización (o ubicación) geográfica"), y desactivar y administrar el historial web (ver apartado "5.22.1.5. Historial de actividad web"):



1119. En caso de habilitar la posibilidad de compartir información actualizada con otros usuarios sobre viajes y desplazamientos (desaconsejado desde el punto de vista de seguridad y privacidad), opción disponible tras la información de la cuenta de Google, debe siempre restringirse, estableciendo qué conjunto de usuarios podrán ver tú ubicación a través de Google+:



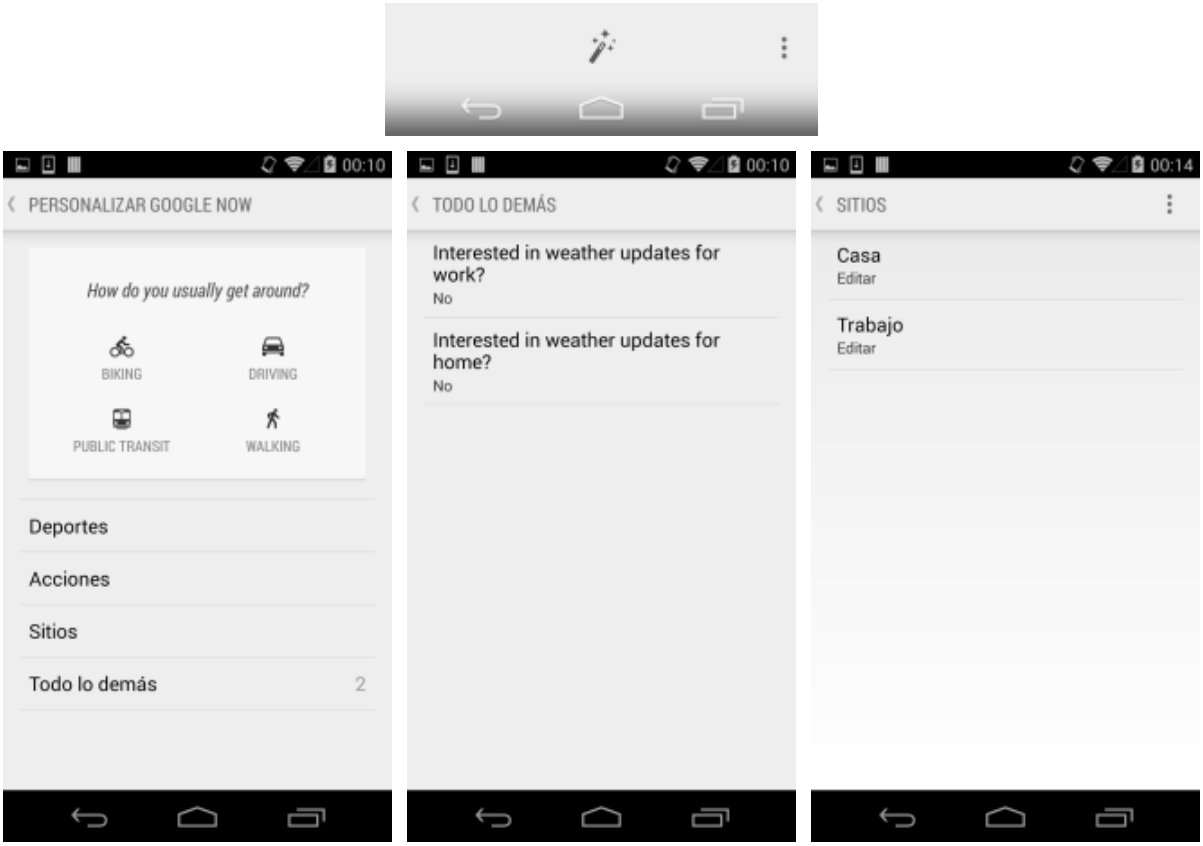
1120. Adicionalmente se dispone de una opción de configuración para recopilar estadísticas de búsqueda de apps en Google Play (habilitada por defecto), y mejorar así las funciones de sugerencias y resultados al realizar estas búsquedas. Esta funcionalidad pueden ser deshabilitada mediante el menú "Estadísticas de búsqueda de aplicaciones locales" y el botón "[SI | NO]", así como borrar las estadísticas ya recopiladas sobre búsqueda de apps:



1121. Por otro lado, la opción "Buscar en google.com" permite definir si se desea usar el dominio local para las búsquedas, es decir, el dominio del país, como por ejemplo "www.google.es", y la opción "Filtro SafeSearch" (deshabilitado por defecto) permite hacer uso de este filtro durante las búsquedas.

1122. El filtro SafeSearch permite bloquear imágenes y vídeos con contenido sexual explícito, así como resultados que puedan dirigir a contenido explícito, de los resultados de las búsquedas de Google, evitando la mayor parte del contenido para adultos [Ref.- 163].

1123. El usuario no tiene control sobre qué tarjetas Google Now se muestran en un momento determinado[99]. Sin embargo, desde la app "Google", empleando el icono con una varita mágica disponible en la parte central inferior, es posible personalizar Google Now y las preferencias de las tarjetas que se quieren ver[100], como por ejemplo deportes (pudiéndose añadir equipos en los que el usuario está interesado), acciones de bolsa (pudiéndose añadir valores bursátiles), sitios o lugares (definiendo dónde se encuentra el trabajo, el sitio al que hay que ir todos los días, y la casa, para obtener información sobre viajes, del usuario), y otros ("Todo lo demás": actualizaciones meteorológicas para el trabajo y para casa). Asimismo se puede indicar como se desplaza el usuario habitualmente (bici, conduciendo, transporte público o andando), y cambiarlo posteriormente desde "Todo lo demás":



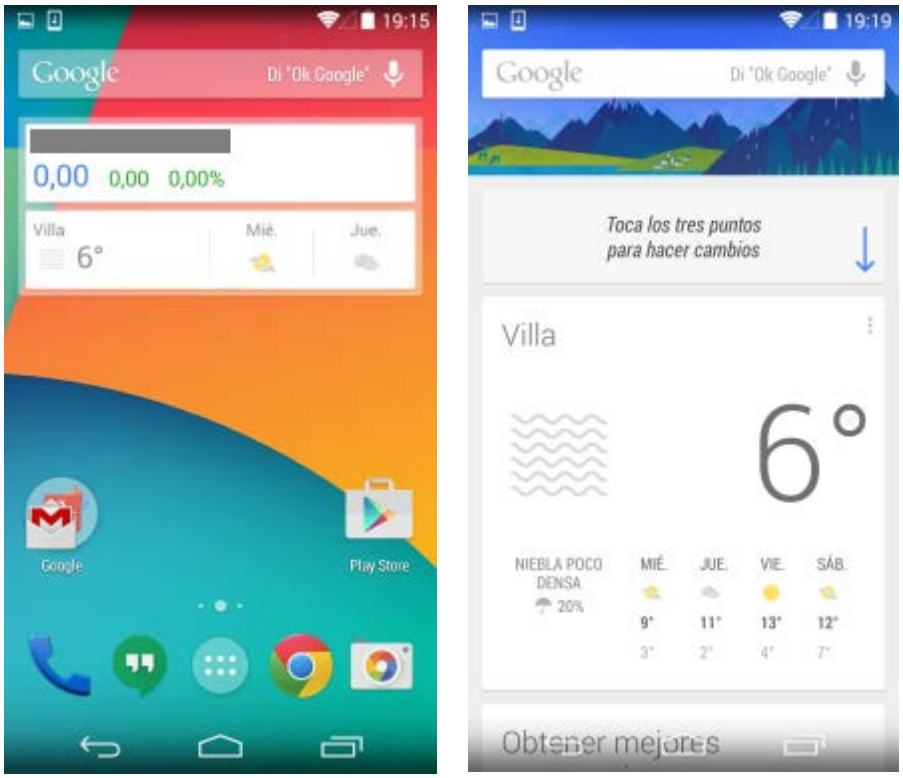
1124. Independientemente a Google Now, la funcionalidad de los servicios de ubicación, el historial de ubicaciones, y el historial web, pueden ser deshabilitados sin desactivar Google Now (pero lógicamente se limitarán las capacidades de este servicio).

5.21.1 GOOGLE EXPERIENCE LAUNCHER

1125. Google Experience Launcher es un servicio qué permite al usuario interactuar con el dispositivo móvil Android mediante la voz, por ejemplo para realizar búsquedas de información a través de Google, y que se encuentra actualmente integrado en Google Now y en la app "Google", asociada al buscador de Google.

[99] https://support.google.com/websearch/answer/2819496
[100] https://support.google.com/websearch/answer/2819541

1126. Google Experience Launcher está disponible desde la parte superior de las pantallas principales o de inicio (en adelante referidas como pantallas de inicio), representado por un campo de búsqueda y un icono con forma de micrófono [Ref.- 177]:

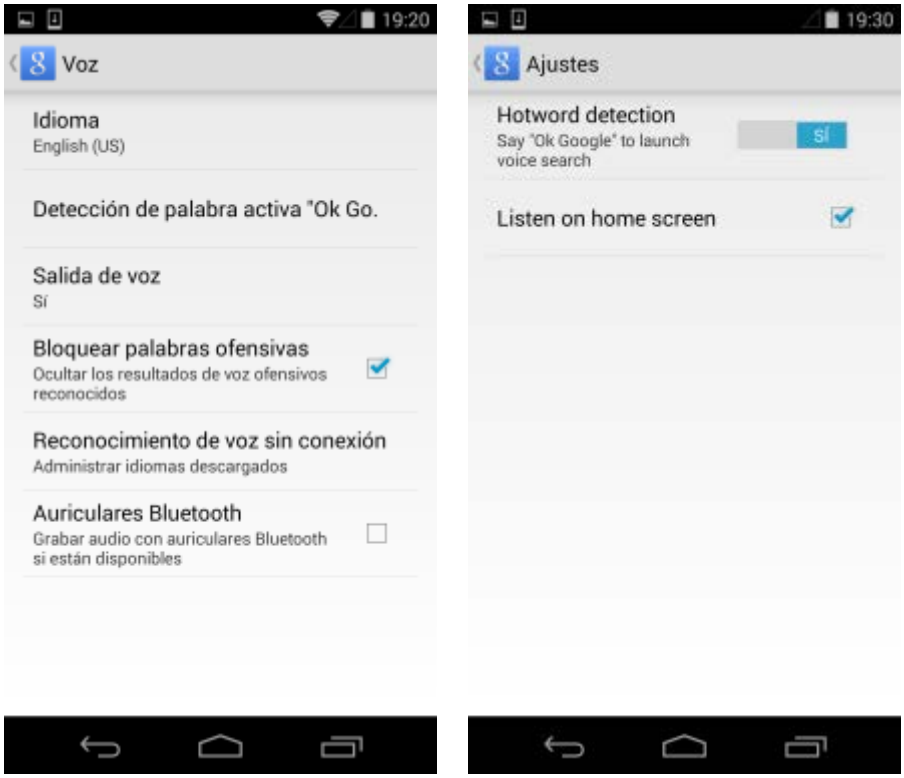


1127. En el caso de estar habilitado, al lado del icono con forma de micrófono aparecerá el texto "Di "Ok Google"", qué permite al usuario comenzar a interactuar con esta funcionalidad mediante la voz y la pronunciación de esa frase ("Ok Google").

1128. Google Experience Launcher está permanentemente activo, siempre que el usuario se encuentre con el dispositivo móvil desbloqueado y en las pantallas de inicio, escuchando al usuario a través del micrófono del dispositivo móvil, y esperando a que se pronuncie la frase de activación ("Ok Google").

1129. El dispositivo móvil no enviará ningún dato a Google mientras permanece en el modo de escucha pasiva, teniendo lugar todo el procesamiento de voz localmente en el dispositivo móvil. Tan pronto el usuario pronuncia la frase de activación, se establece una conexión mediante HTTPS con los servidores de Google para interpretar las indicaciones de voz del usuario al realizar una búsqueda o ejecutar una acción, y obtener los resultados desde los servidores de Google.

1130. Esta funcionalidad puede ser deshabilitada desde la app "Google", y en concreto, desde el botón de menú, a través de la opción "Ajustes", desde dónde es posible acceder a los ajustes de Google Now (y de la app "Google"). La sección "Voz" permite mediante la opción "Detección de palabra activa "Ok Google"", y del botón "[SI | NO]" asociado a la opción "Hotword detection", activar o desactivar esta funcionalidad:

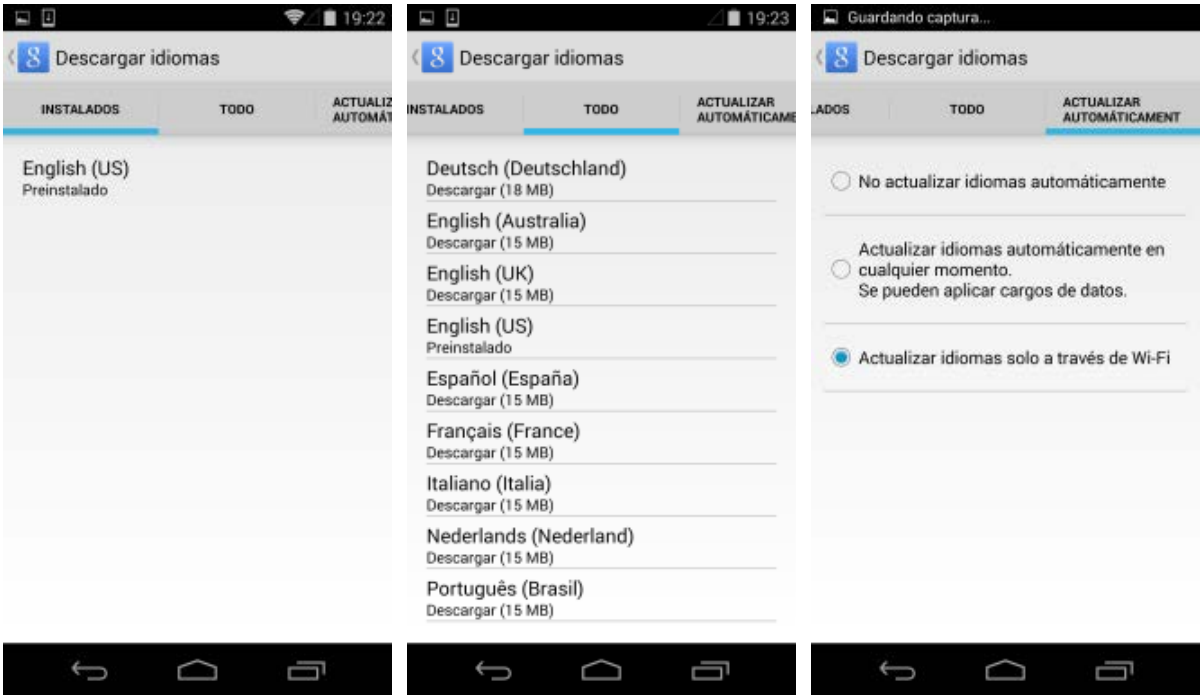


1131. En caso de estar activa (opción habilitada por defecto), es posible determinar si el dispositivo móvil estará escuchando permanentemente en las pantallas principales o de inicio, mediante la opción "Listen on home screen"[101] (habilitada por defecto).

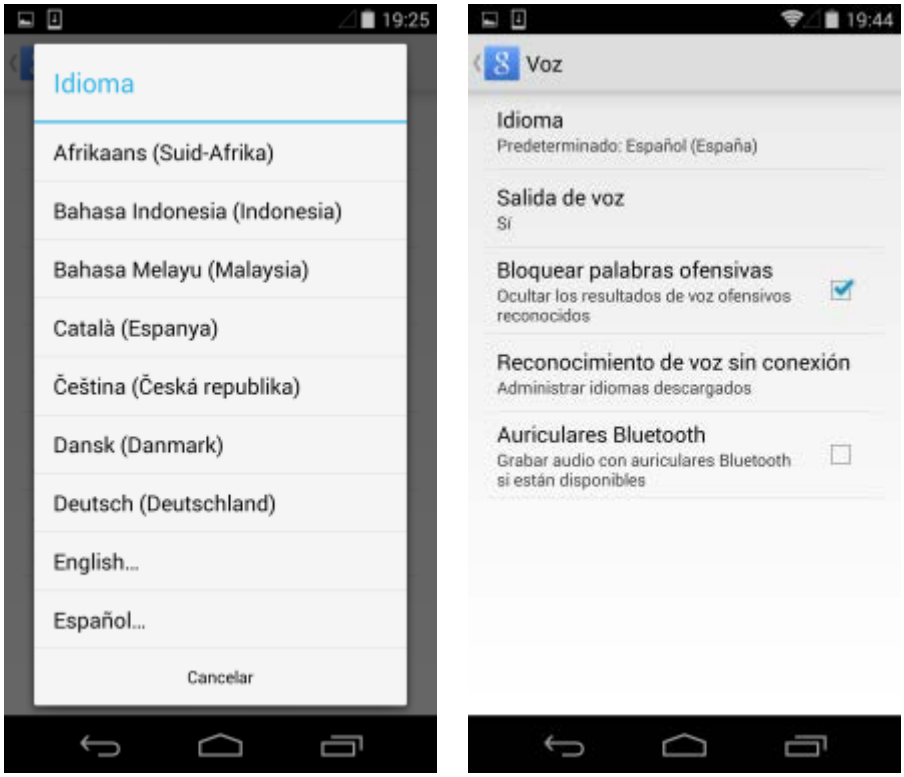
1132. Si se deshabilita la opción "Hotword detection", aún es posible hacer uso de esta funcionalidad pulsando manualmente el icono del micrófono, para iniciar una búsqueda. Si también se deshabilita la opción de escuchar en las pantallas de inicio, el resultado es el mismo, y sólo es posible hacer uso de esta funcionalidad pulsando el icono del micrófono.

1133. Adicionalmente, mediante la modificación de los ajustes de la app "Google" también es posible deshabilitar de forma efectiva su utilización. Por defecto, la app "Google" dispone del idioma "English (US)" preinstalado. Desde el botón de menú, y la opción "Ajustes", es posible acceder a los ajustes de Google Now (y de la app "Google"). La sección "Voz" permite seleccionar el idioma a emplear (opción "Idioma"), mientras que la opción "Reconocimiento de voz sin conexión" permite administrar los idiomas descargados (ver imágenes superiores e inferiores):

[101] Como se puede ver, estas opciones de configuración no han sido traducidas en Android del inglés.



1134. Si sólo se dispone en el dispositivo móvil del idioma existente o preinstalado por defecto, "English (US)", y el idioma se fija a otro valor diferente, por ejemplo "Español (España)", la funcionalidad de Google Experience Launcher estará desactivada, y desaparecerá el texto "Di "Ok Google"" del campo de búsqueda superior de las pantallas principales o de inicio:



1135. Desde la opción "Descargar idiomas" es posible configurar si se desea que se descarguen y actualicen los ficheros de reconocimiento de idiomas, a través de la pestaña "Actualizar Automáticamente". Por defecto, la opción seleccionada es "Actualizar idiomas solo a través de Wi-Fi" (ver imágnes superiores).

1136. La opción "Salida de voz" (activa por defecto) permite configurar si se recibirá una respuesta audible para las búsquedas realizadas.

1137. Desde el punto de vista de seguridad se recomienda no habilitar la funcionalidad de Google Experience Launcher, salvo que se quiera hacer uso explícito de la misma.

5.22 APLICACIONES MÓVILES (APPS) EN ANDROID

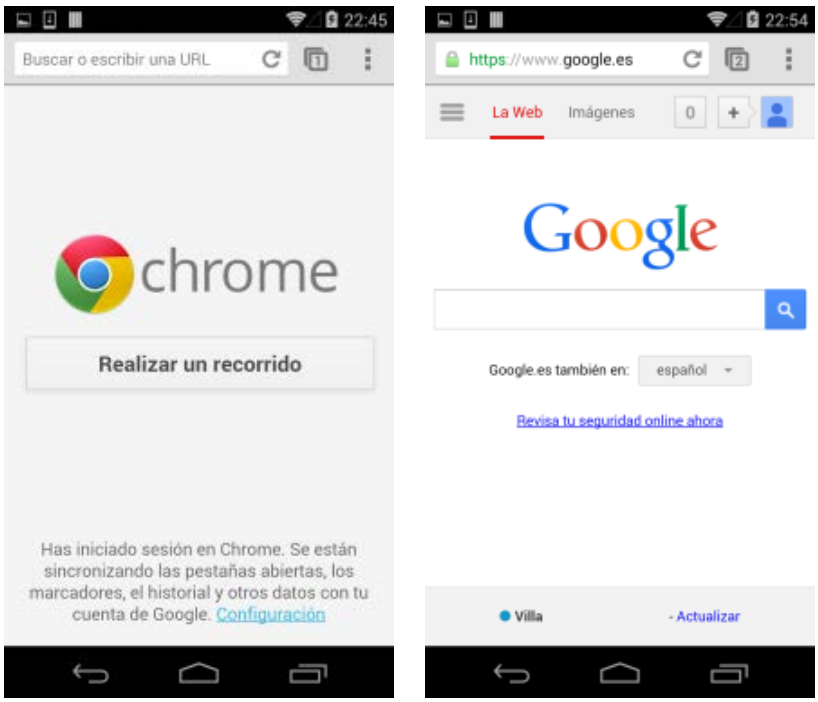
1138. Los siguientes apartados proporcionan breves recomendaciones de seguridad asociadas a las aplicaciones más comunes y relevantes existentes por defecto en Android. En ningún caso se pretende realizar un análisis de seguridad exhaustivo de su funcionamiento y de todas las opciones de configuración disponibles en cada app.

Nota: el número de aplicaciones móviles instaladas por defecto en Android por Google, el fabricante del dispositivo móvil o el operador de telefonía móvil, así como la variedad de apps de otras compañías que pueden ser instaladas posteriormente manualmente o desde Google Play, hace inviable su análisis de seguridad dentro del alcance de la presente guía.

Para todas las apps instaladas, o a instalar, en el dispositivo móvil se recomienda realizar una análisis detallado, identificando la versión actualmente instalada, evaluando la gestión de credenciales de acceso (almacenamiento y utilización), así como los protocolos empleados durante el proceso de autentificación y durante el resto de la sesión, y las capacidades de cifrado, tanto para el envío y recepción de datos, como para el almacenamiento de los mismos localmente, junto a cualquier otra característica de seguridad ofrecida por la app.

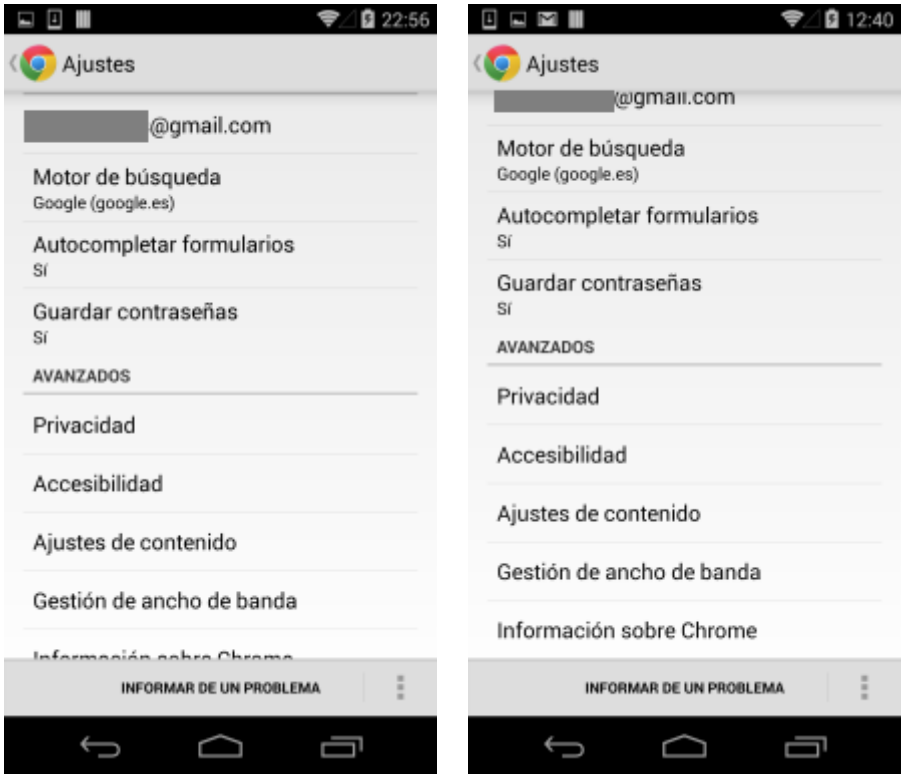
5.22.1 NAVEGACIÓN WEB: NAVEGADOR CHROME

1139. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. Android, a partir de la versión 4.3, incluye por defecto el navegador web Chrome y disponible desde el *Launcher*, basado en el motor de código abierto WebKit y en el motor JavaScript Chrome V8.



1140. Chrome sustituye al navegador web existente previamente por defecto en versiones anteriores de Android, que presentaba carencias de seguridad significativas, tal y como se describe en la versión previa de la presente guía para Android 2.x [Ref.- 130] y con algunas referencias breves en los siguientes apartados (como por ejemplo “5.22.1.7. Android WebViews”).

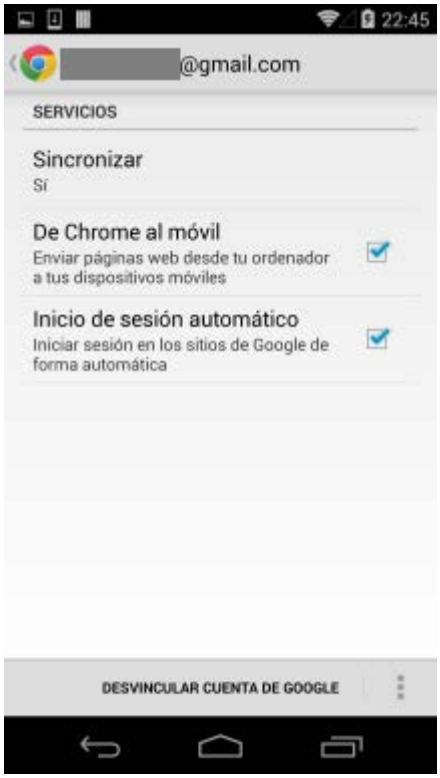
1141. A través del botón "Menú", cuando la app de Chrome está siendo ejecutada, es posible acceder mediante la opción "Ajustes" al menú de configuración de Chrome, desde dónde se pueden (entre otros) gestionar múltiples ajustes, tanto "[Básicos]" como "[Avanzados]":



1142. La versión de Chrome disponible por defecto en Android 4.4.4 es la versión 32.0.1700.99.

1143. Chrome soluciona algunas de las limitaciones de seguridad relevantes existentes en el navegador web de Android disponible por defecto en versiones previas del sistema operativo, como por ejemplo contar con soporte para cookies "HttpOnly", empleadas para proteger la sesión de un usuario frente a ataques de Cross-Site Scripting (XSS) [Ref.- 121].

1144. Mediante la selección de la cuenta de usuario de Google es posible definir si se hará uso del servicio de sincronización de datos de Chrome (habilitado por defecto) que permite sincronizar las pestañas abiertas en el navegador, los favoritos o marcadores, el historial de navegación, la información para autocompletar formularios, e incluso las contraseñas, entre el dispositivo móvil y un ordenador [Ref.- 64]:



1145. Pulsando la opción "Sincronizar" es posible especificar individualmente qué tipos de datos serán sincronizados entre el dispositivo móvil y el ordenador:

1146. En caso de requerir hacer uso de esta funcionalidad, se recomienda restringir y minimizar el tipo de datos que serán sincronizados, especialmente, las contraseñas.

1147. Una opción crítica desde el punto de vista de seguridad y la sincronización de Chrome es la asociada a la opción "Encriptación". Ésta permite dos opciones, "Encriptar

contraseñas con credenciales de Google" (habilitada por defecto), cifrándose las contraseñas con las credenciales de la cuenta de usuario de Google, o "Encriptar todo con contraseña", opción que permite al usuario establecer una contraseña para acceder a los datos sincronizados:

1148. La opción recomendada desde el punto de vista de seguridad es no sincronizar las contraseñas mediante este servicio. En caso de hacerlo, se debe hacer uso de la opción "Encriptar todo con contraseña", empleando una contraseña independiente y diferente de la asociada a las credenciales de la cuenta de usuario de Google, y , especialmente haciendo uso de una frase de paso o *passphrase*, es decir, una contraseña suficientemente larga y robusta [Ref.- 64].

1149. La opción "De Chrome al móvil" (habilitada por defecto) permite enviar páginas web desde un ordenador que haga uso del navegador web Chrome al dispositivo móvil.

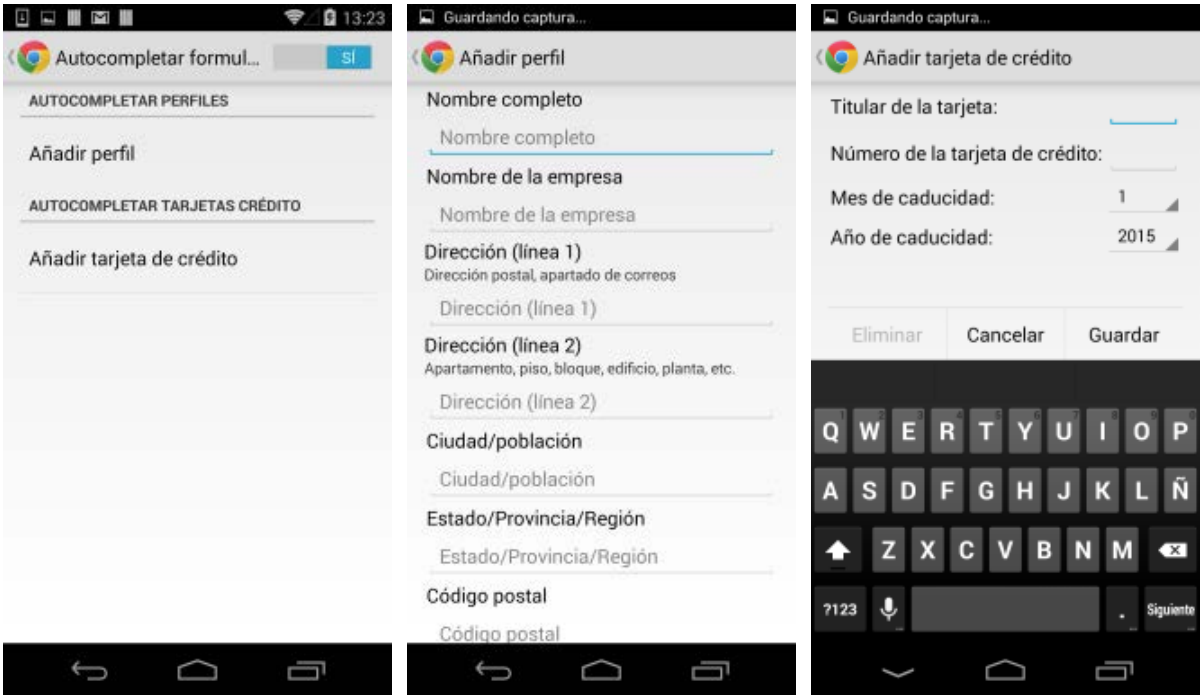
1150. La opción "Inicio de sesión automático" permite a Chrome iniciar una sesión con las credenciales asociadas a la cuenta de usuario de Google en los sitios web de Google de forma automática y sin la intervención del usuario.

1151. Desde el punto de vista de seguridad, se recomienda deshabilitar ambas opciones para evitar que exista la transferencia de datos de sincronización descrita (salvo que se desee hacer un uso explícito de esta funcionalidad), y que el usuario sea consciente de cuando se debe autentificar en los servicios de Google.

1152. El botón "Desvincular cuenta de Google" (situado en la parte inferior) permite al usuario hacer uso de Chrome sin que éste esté asociado a una cuenta de usuario de Google, es decir, de manera más anónima e independiente.

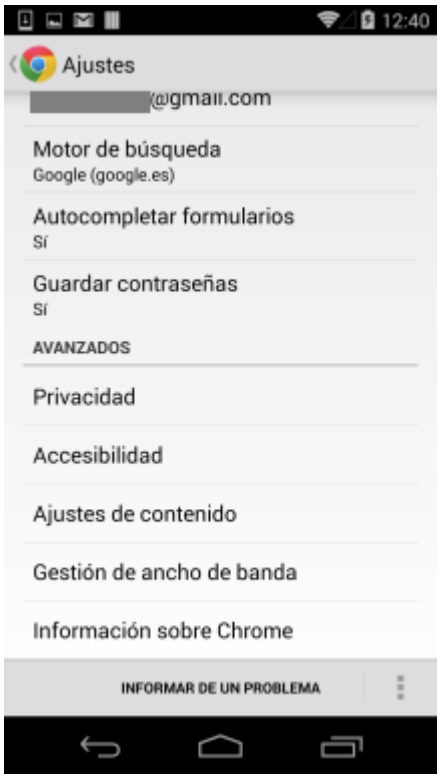
1153. Mediante la opción "Autocompletar formularios" (habilitada por defecto) se permite a Chrome autocompletar formularios con la información del perfil de usuario especificada (por defecto no se dispone de ningún perfil, y éste debe ser añadido con los datos de contacto del usuario) y autocompletar la información de tarjetas de crédito con la

información especificada (por defecto no se dispone de ninguna tarjeta de crédito, y ésta debe ser añadida manualmente):



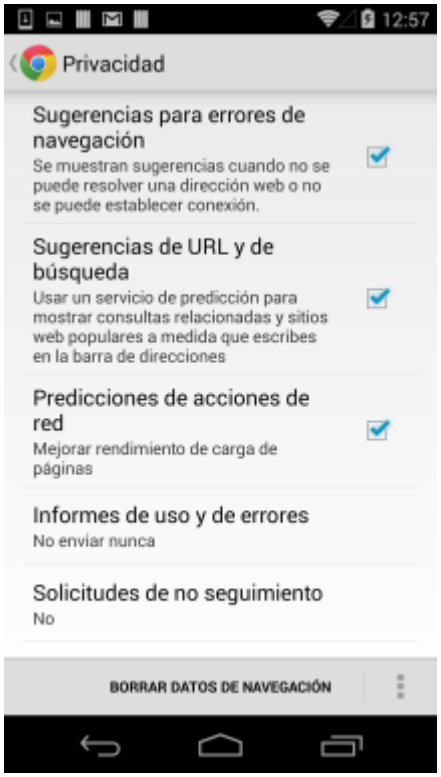
1154. Se recomienda deshabilitar esta opción y no recordar los datos introducidos en formularios. En caso de existir información sobre el perfil del usuario o tarjetas de crédito, se recomienda borrar los datos almacenados actualmente.

1155. Mediante la opción "Guardar contraseñas" (habilitada por defecto) se permite a Chrome almacenar las contraseñas utilizadas por el usuario al autentificarse en sitios web:

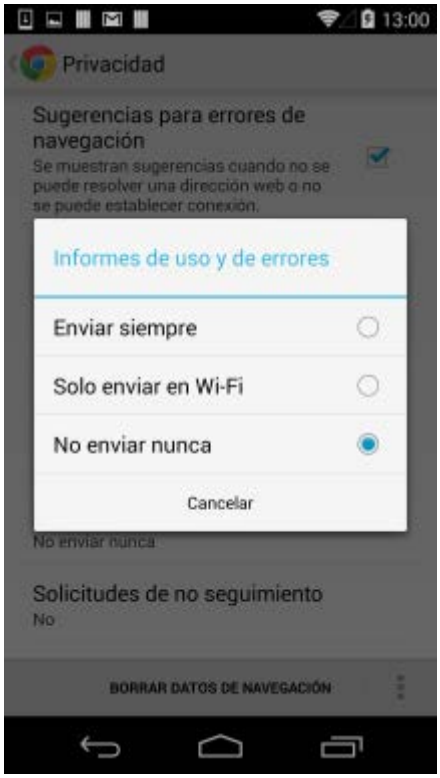


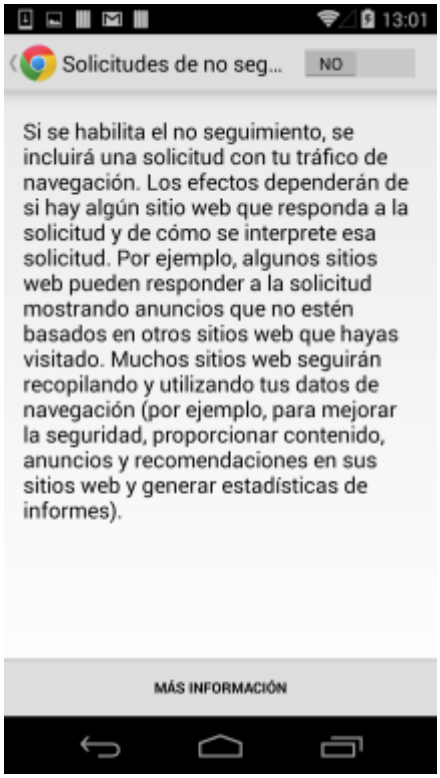
1156. Se recomienda deshabilitar esta opción y no recordar las contraseñas, debiendo eliminar las que están almacenadas actualmente (posteriormente se indica cómo eliminar los datos actuales de manera global a través de la opción "Historial").

1157. Desde la sección "Privacidad", se pueden obtener sugerencias al presentarse errores de navegación, sugerencias de URLs y búsquedas, y mejorar la carga de páginas web mediante las predicciones de acciones de red. Todas estas opciones están habilitadas por defecto:



1158. Adicionalmente se dispone de opciones para el envío de informes de uso y errores y de solicitudes de no seguimiento (deshabilitada por defecto):



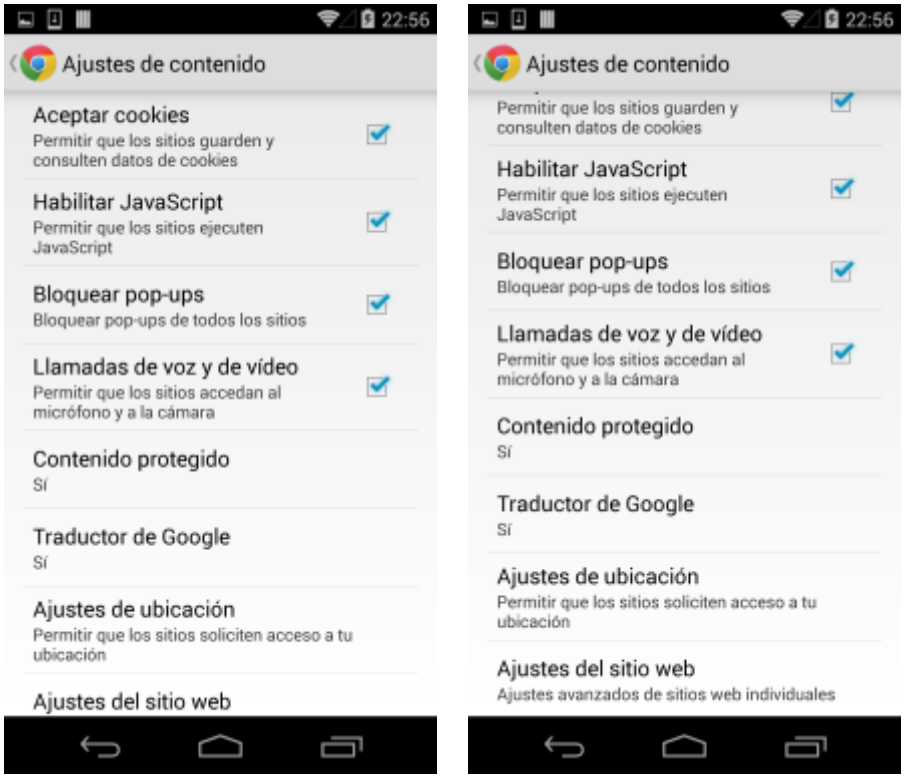


1159. Desde el punto de vista de la privacidad del usuario, se recomienda deshabilitar todas las opciones de sugerencias y predicciones descritas.

1160. Asimismo, se recomienda no enviar nunca informes de uso y errores, y habilitar las solicitudes de no seguimiento, para que el navegador web añada en sus peticiones la cabecera HTTP "DNT: 1" (Do Not Track, DNT) indicando a los sitios web visitados que no quiere ser monitorizado (el resultado de este ajuste de configuración depende únicamente del comportamiento de los sitios web visitados, que pueden tener en cuenta dicha cabecera, o hacer caso omiso de la misma).

1161. Las opciones de "Accesibilidad" no deberían tener un impacto directo en la seguridad del dispositivo móvil.

1162. Desde la sección "Ajustes de contenido" es posible aceptar el uso de cookies (habilitado por defecto), habilitar JavaScript (habilitado por defecto), bloquear pop-ups (habilitado por defecto), permitir la realización de llamadas de voz y vídeo, funcionalidad para la que los sitios web deben acceder al micrófono y la cámara del dispositivo móvil (habilitado por defecto), activar la protección de contenido necesaria para la reproducción de música y vídeos *premium* y/o protegidos por *copyright* (habilitado por defecto), activar el traductor de Google (habilitado por defecto), y acceso a los ajustes de ubicación (ver apartado "5.10. Localización (o ubicación) geográfica") y del sitio web:

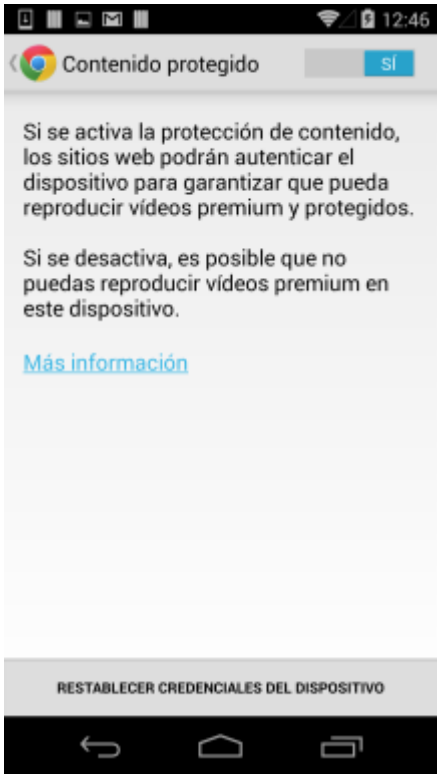


1163. Para una navegación web más segura, pero muy restringida desde el punto de vista de su funcionalidad, se recomienda deshabilitar la ejecución de scripts (JavaScript), mediante la opción "Habilitar JavaScript", y el uso de cookies en el navegador web, mediante la opción "Aceptar cookies", con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador web y a la privacidad del usuario a través de las cookies. Adicionalmente, el bloqueo de pop-ups es una opción que debe estar habilitada.

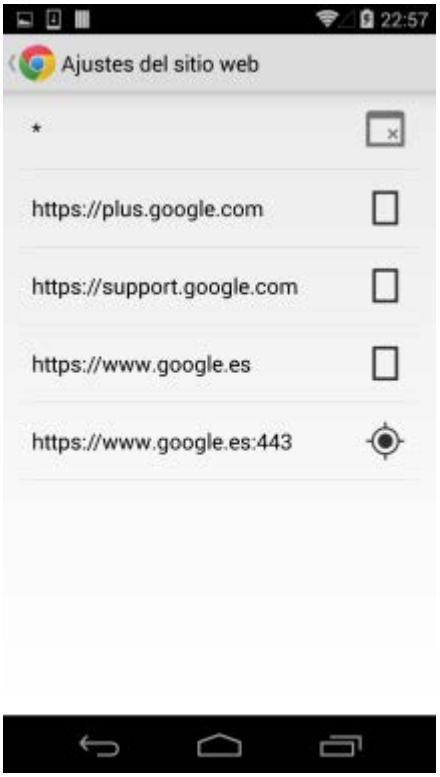
1164. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts y cookies en sus contenidos web y para su funcionamiento (la mayoría de páginas web en Internet), por lo que puede ser necesario tener que dejar habilitadas ambas opciones.

1165. Se recomienda deshabilitar la opción "Llamadas de voz y vídeo" para no permitir el acceso al micrófono y la cámara del dispositivo móvil a los sitios web.

1166. La opción "Contenido protegido" permite a sitios web como Netflix o Google Play autentificar al dispositivo móvil para confirmar si dispone de permisos para acceder a contenidos protegidos por *copyright*. Salvo que se haga un uso explícito de este tipo de contenido, se recomienda deshabilitar esta opción:

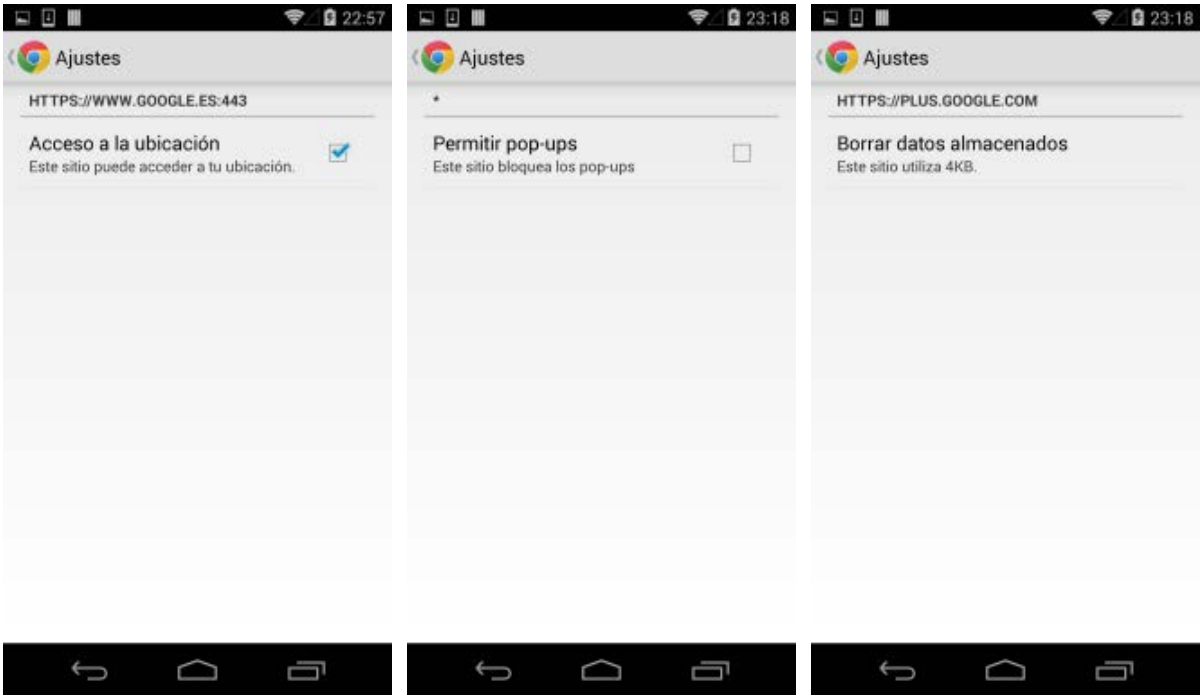


1167. Los "Ajustes del sitio web", accesibles al igual que las secciones previas desde la pantalla de "Ajustes [Avanzados] - Ajustes de contenido" de Chrome, permiten obtener una lista de sitios web visitados, y gestionar los permisos otorgados a cada uno de ellos individualmente. Cada uno de estos elementos puede ser eliminado individualmente:

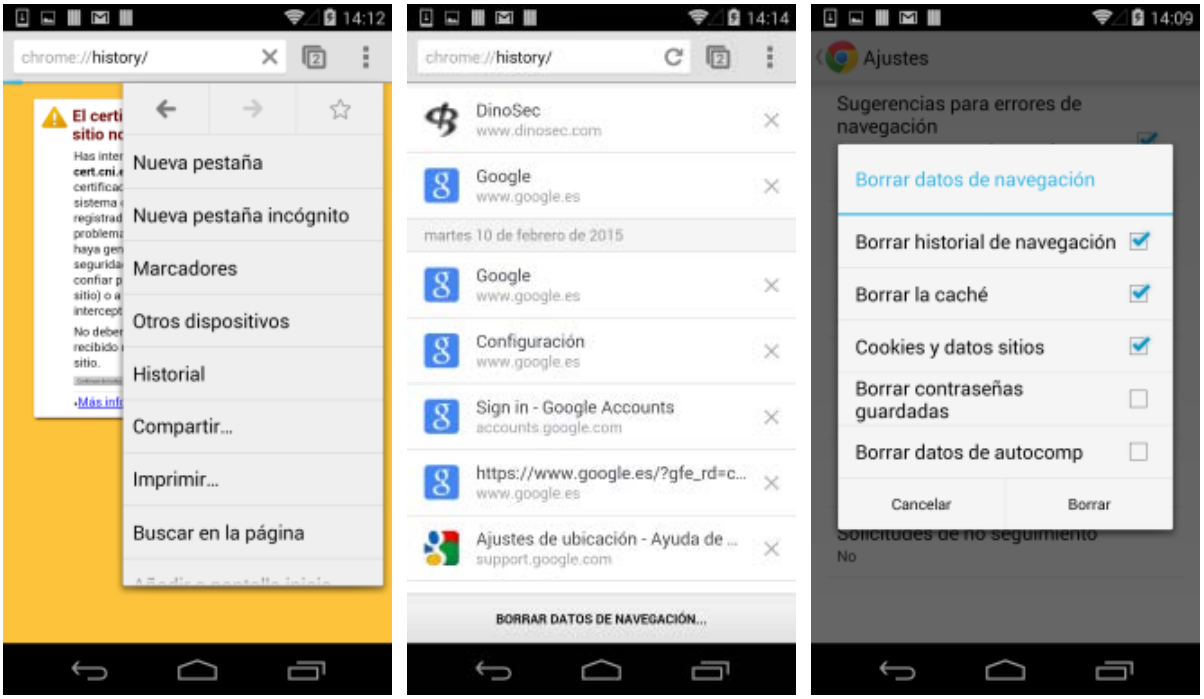


1168. Esta sección contiene un listado de sitios web con ajustes avanzados de configuración para sitios web específicos, como por ejemplo si se permiten pop-ups para todos los sitios web (identificados con el carácter comodín, "*"), o la posibilidad de borrar los datos

almacenados en caché para un sitio web concreto, aparte de las capacidades de habilitar o deshabilitar el acceso a la ubicación (ver apartado "5.10.6.7. Navegador web"):

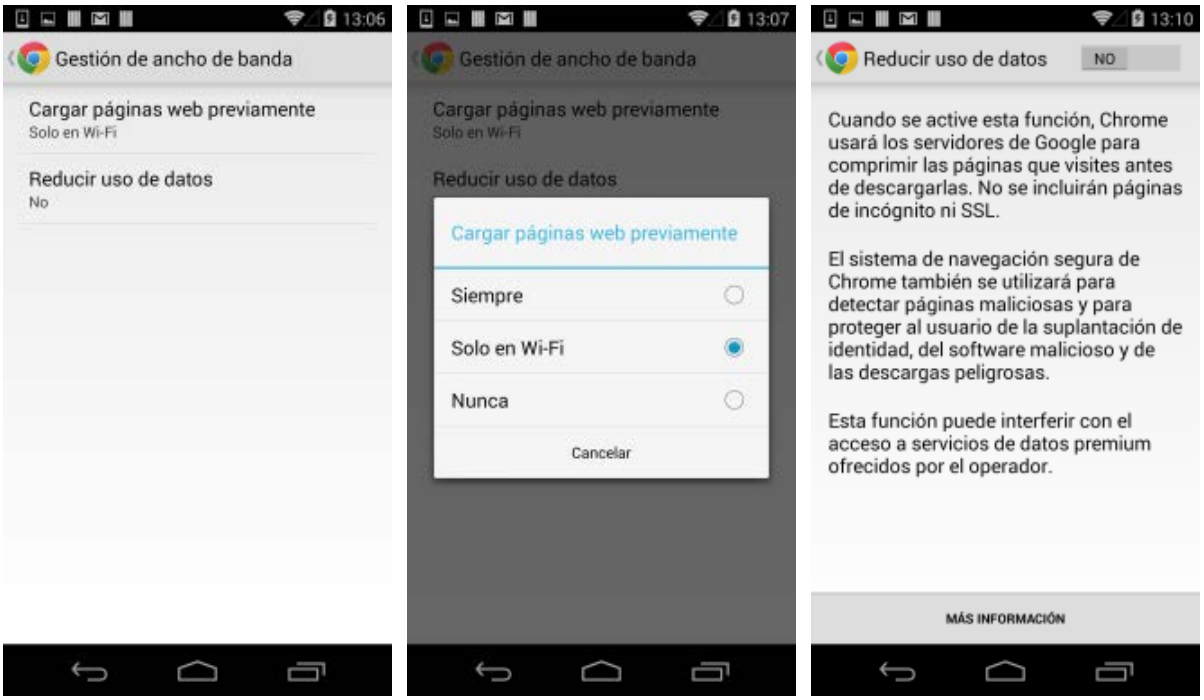


1169. Por otro lado, y en lugar de hacerlo de forma individual por cada sitio web, desde el menú "Historial" de Chrome (fuera del menú de "Ajustes") es posible borrar los datos de navegación de manera global, mediante la opción "Borrar datos de navegación":



1170. Estos datos incluyen el historial de navegación, la caché, las cookies y otros datos almacenados por los sitios web, las contraseñas y los datos para autocompletar formularios, almacenados actualmente.

1171. Desde la sección "Gestión de ancho de banda", se permite habilitar la carga previa de páginas web para acelerar la navegación (habilitada por defecto sólo en Wi-Fi) y reducir el uso de datos (deshabilitado por defecto):



1172. No se recomienda habilitar la opción "Reducir uso de datos", ya que ésta implica que al navegar a diferentes sitios web, Chrome enviará las peticiones a través de los servidores de Google para que estos compriman los contenidos antes de descargarlos. Es decir, Google podría disponer de todos los detalles sobre las páginas web visitadas por el usuario, excepto para las páginas web accedidas mediante HTTPS o desde una pestaña de incógnito. Aunque esta funcionalidad también ofrece otros mecanismos de protección, como por ejemplo la detección de páginas con contenido malicioso, o involucradas en esquemas de suplantación de identidad, se desaconseja su utilización ya que el impacto sobre la privacidad del usuario al habilitarla es muy elevado.

1173. Desde el punto de vista de seguridad y privacidad del usuario, se sugiere aplicar las recomendaciones descritas previamente para cada sección con el objetivo de limitar la exposición del dispositivo móvil durante las actividades de navegación web.

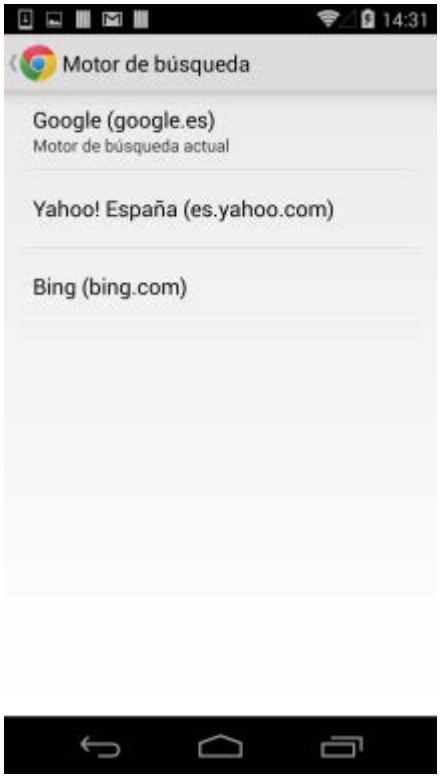
1174. Se recomienda borrar de forma frecuente (tanto globalmente, como de forma individual para ciertos sitios web específicos, según las necesidades del usuario) tanto la caché como el historial de navegación web, así como el almacenamiento de cookies, y datos de formularios y contraseñas, con el objetivo de proteger la privacidad del usuario.

5.22.1.1 PROVEEDOR DE BÚSQUEDAS AUTOMÁTICO

1175. Cuando se introduce un término en la barra de navegación del navegador web, si éste no corresponde con un servidor web, de forma automática se realiza una búsqueda de dicho término a través del buscador de Google (www.google.com)[102].

1176. El proveedor de búsquedas a emplear está disponible a través del menú de "Ajustes" de Chrome y la opción "Motor de búsqueda" (por defecto, Google):

[102] También puede emplearse la versión localizada del buscador de Google según el país: "www.google.es".



1177. Este comportamiento tiene implicaciones de seguridad relevantes al revelar (potencialmente) en Internet la información introducida en la barra de navegación, como por ejemplo el nombre de servidores internos de una organización[103].

1178. Adicionalmente, la información del dispositivo móvil se desvela en los parámetros de la URL de "www.google.com" empleada para las búsquedas, incluyendo referencias a Chrome para Android, es decir, del navegador web y del tipo de plataforma móvil:

```
GET  /search?q=siles&oq=siles&aqs=chrome.0.69i59j69i60&client=ms-android-
   google&sourceid=chrome-mobile&espv=1&ie=UTF-8 HTTP/1.1
Host: www.google.es
```

5.22.1.2 IDENTIFICACIÓN DEL NAVEGADOR WEB

1179. Cuando el navegador web accede a Internet, por ejemplo al buscador de Google, la cadena de caracteres que identifica al navegador web o agente de usuario (User-Agent) tiene el siguiente valor, revelando excesivos detalles sobre la versión del navegador web y la plataforma:

```
User-Agent: Mozilla/5.0 (Linux; Android 4.4.4; Nexus 5 Build/KTU84P)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.99 Mobile
Safari/537.36
```

1180. Los detalles del dispositivo móvil incluyen la plataforma ("Android"), la versión de Android ("4.4.4"), el modelo de terminal ("Nexus 5"), la versión de compilación de

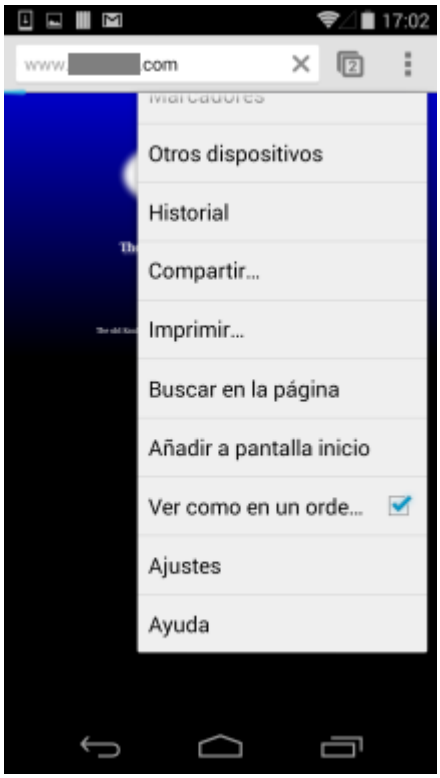
[103] En función de la versión de Android y del navegador, podría desvelarse el término introducido carácter a carácter según la palabra es tecleada (no es el caso de la versión de Chrome por defecto en Android 4.4.4).

Android ("KTU84P"), o los detalles del navegador web (incluyendo su versión exacta y múltiples versiones de sus componentes).

1181. Se recomienda modificar el valor del agente de usuario para que no desvele información adicional. Desde el botón de menú, es posible hacer uso de la opción "Ver como en un ordenador" para forzar a Chrome a usar un agente de usuario distinto, similar al empleado por un ordenador:

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/32.0.1700.99 Safari/537.36
```

1182. Este agente de usuario emula la utilización del navegador web Chrome sobre un ordenador Linux genérico, incluyendo de nuevo los detalles del navegador web (como por ejemplo, su versión exacta):



1183. Adicionalmente, las peticiones web pueden desvelar otros detalles sensibles a través de cabeceras HTTP adicionales, como por ejemplo el uso de Chrome (a través de la cabecera "X-Chrome-Variations") o incluso detalles de la ubicación del usuario (a través de la cabecera "X-Geo" en base64), que corresponde a la siguiente cadena de caracteres, "role:1 producer:12 timestamp:1424092822777000 latlng{latitude_e7:400000002 longitude_e7:-40000001} radius:53287", dónde entre otros se puede obtener los valores de latitud y longitud:

```
X-Geo:
cm9sZToxIHByb2R1Y2VyOjEyIHRpbWVzdGFtcDoxNDI0MDkyODIyNzc3MDAwIGxhdGxuZ3tsY
XRpdHVkZV9lNzo0MDAwMDAwMDIgbG9uZ2l0dWRlX2U3Oi00MDAwMDAwMX0gcmFkaXVzOjUzMj
g3
X-Chrome-Variations: CKa2yQEZVbbJAQ==
```

1184. Se recomienda evaluar si habitualmente se desea realizar la navegación web como un ordenador o equipo de sobremesa (opción recomendada desde el punto de vista de seguridad para no desvelar los detalles reales del dispositivo móvil), más expuesto a ataques genéricos sobre todas las versiones del navegador web pero que probablemente no tengan éxito en el dispositivo móvil, o como dispositivo móvil, más expuesto a ataques dirigidos a este tipo de terminales y con posibilidad mayor de éxito.

1185. Debe tenerse en cuenta que la modificación del agente de usuario, y especialmente el valor de la plataforma (tradicional o móvil), podría afectar a la presentación de los contenidos web de ciertos servidores y aplicaciones web que personalizan las respuestas en función de si el cliente es un dispositivo móvil o un ordenador (de sobremesa o portátil).

Nota: la modificación o eliminación de información de las cabeceras HTTP puede afectar a la funcionalidad de servidores y aplicaciones web que hacen uso de dichos datos para procesar y mostrar contenidos web personalizados para el tipo de dispositivo cliente. Estas implicaciones se han mencionado igualmente a lo largo de la presente sección al deshabilitar otras funcionalidades disponibles habitualmente en los navegadores web.

Las recomendaciones de seguridad descritas a lo largo de toda la sección pretenden incrementar el nivel de seguridad y privacidad del dispositivo móvil y de su usuario, pudiendo afectar por tanto a la funcionalidad, por lo que deben ser aplicadas únicamente si no es necesario hacer uso de la funcionalidad asociada.

1186. Algunos módulos de navegación web de Android, como el asociado a la información del GPS y gpsOneXTRA (ver apartado "5.10.4. gpsOneXTRA"), añaden la siguiente cabecera WAP que permite identificar el tipo de terminal (fabricante y modelo):

```
x-wap-profile:
    http://www.openmobilealliance.org/tech/profiles/UAPROF/ccppschema-
    20021212#
```

1187. El UAProf (*User-Agent Profile*) es un documento XML que contiene información sobre las características y capacidades de un dispositivo móvil, estándar definido por OMA, Open Mobile Alliance. El documento está especificado en las cabecera HTTP "x-wap-profile" (o "Profile"), apuntando normalmente a una web del fabricante del terminal (repositorio de perfiles).

1188. El perfil puede contener información muy detallada del dispositivo móvil, incluyendo los perfiles Bluetooth, los tipos y formatos de datos soportados, protocolos de seguridad y de transferencia de datos soportados, capacidades push, WAP, MMS y de *streaming*.

1189. En el caso de Android el perfil referenciado está asociado a una plantilla genérica para dispositivos móviles definida por la OMA, sin desvelar detalles particulares del terminal.

5.22.1.3 CONTENIDOS ADOBE FLASH

1190. Adobe anunció en noviembre de 2011 que no soportaría Adobe Flash en dispositivos móviles [Ref.- 105], en favor de las tecnologías basadas en HTML 5.

1191. Por este motivo, Adobe Flash no está soportado en el navegador web Chrome para Android [Ref.- 109]. disponible por defecto en esta plataforma móvil.

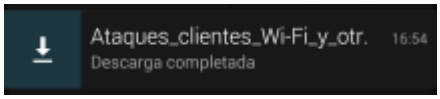
1192. Pese a que otros navegadores web para Android sí pueden disponer de soporte para Flash, como por ejemplo Firefox[104], Boat o Dolphin, desde el punto de vista de seguridad no se recomienda su instalación, ya que la misma se basa en la instalación de versiones antiguas del reproductor de Flash para dispositivos móviles (Adobe Flash Player), para el que con una muy alta probabilidad se conocerán vulnerabilidades existentes públicamente.

1193. Debe tenerse en cuenta que las mejoras de seguridad incorporadas en las últimas versiones de Flash Player para los equipos de escritorio, por ejemplo en la versión 16.x, ya no están disponibles en Flash Player para Android.

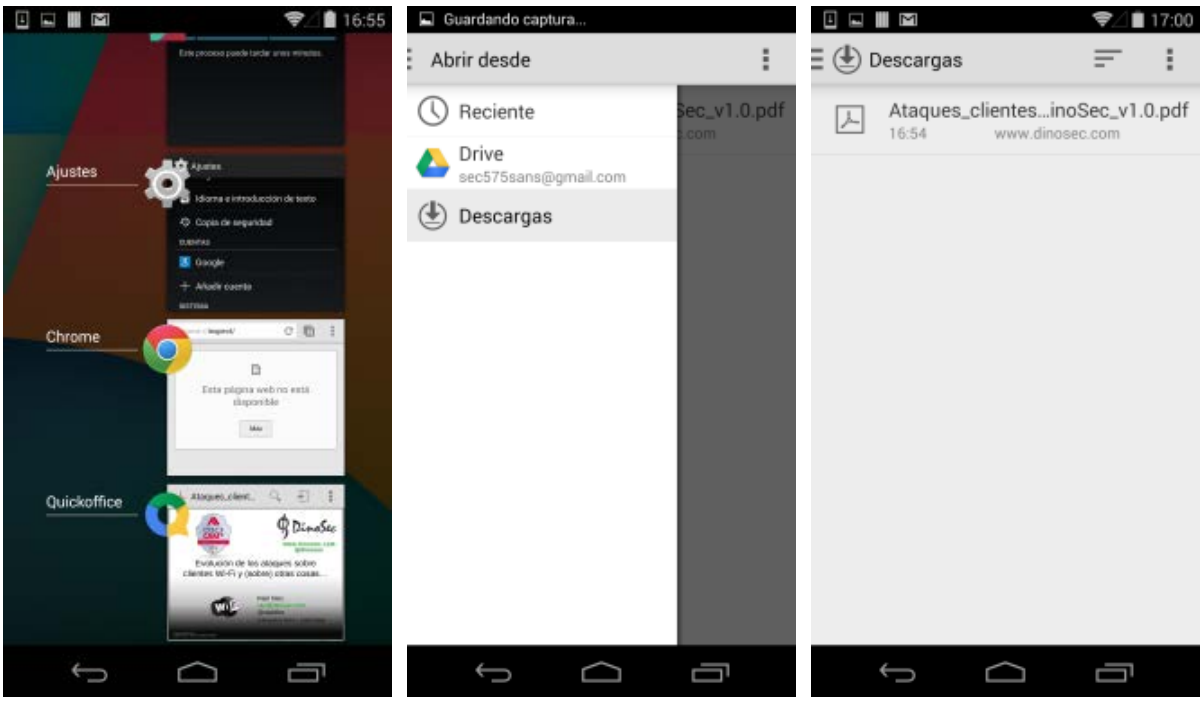
5.22.1.4 CONTENIDOS ADOBE PDF

1194. Android incluye por defecto una app para la lectura de ficheros PDF denominada Quickoffice, versión 6.3.1.041 (disponible por defecto en Android 4.4.4), siendo también posible instalar el cliente oficial Adobe Reader desde Google Play.

1195. Quickoffice está disponible desde el *Launcher* y también al acceder a contenidos PDF desde el navegador web. Chrome descargará el fichero PDF automáticamente (a la carpeta general de "Descargas", o "Download", del almacenamiento interno del dispositivo móvil; ver imágnes siguientes) y el mismo podrá ser accedido también a través de la notificación del navegador web de que el fichero ha sido descargado:



1196. Al seleccionar el fichero PDF, éste será abierto automáticamente mediante Quickoffice:



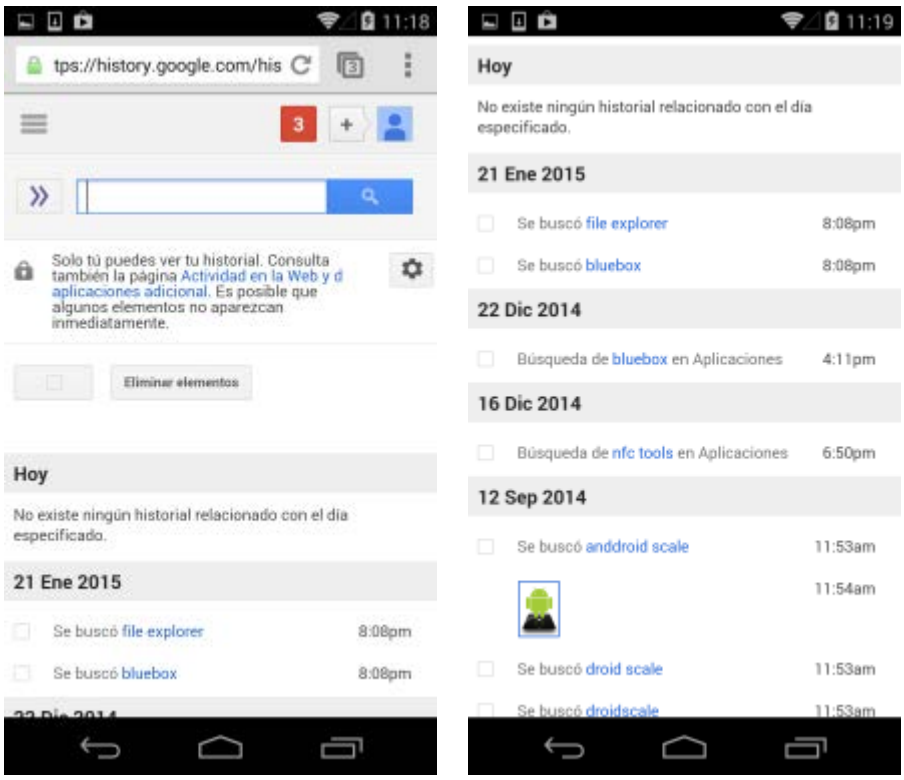
1197. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF (Adobe Acrobat, Adobe Reader, Foxit, etc.) durante los últimos años, se recomienda siempre mantener actualizada la app de visualización de ficheros PDF a la última versión.

[104] https://support.mozilla.org/es/kb/firefox-para-moviles-no-admite-flash

5.22.1.5 HISTORIAL DE ACTIVIDAD WEB Y DE APLICACIONES

1198. Las búsquedas realizadas por el usuario a través de Google, así como la actividad de navegación web y de otras apps, es almacenada en la página "Actividad web y de aplicaciones" de la cuenta de usuario de Google.

1199. La página "Actividad web y de aplicaciones" está disponible a través de la siguiente URL: "https://history.google.com/history". Esta funcionalidad está asociada al "Historial de la cuenta", disponible desde "https://www.google.com/settings/accounthistory" (y que también permite el acceso al historial de ubicaciones, ver apartado "5.10.5. Historial de ubicaciones e informes de ubicación"):



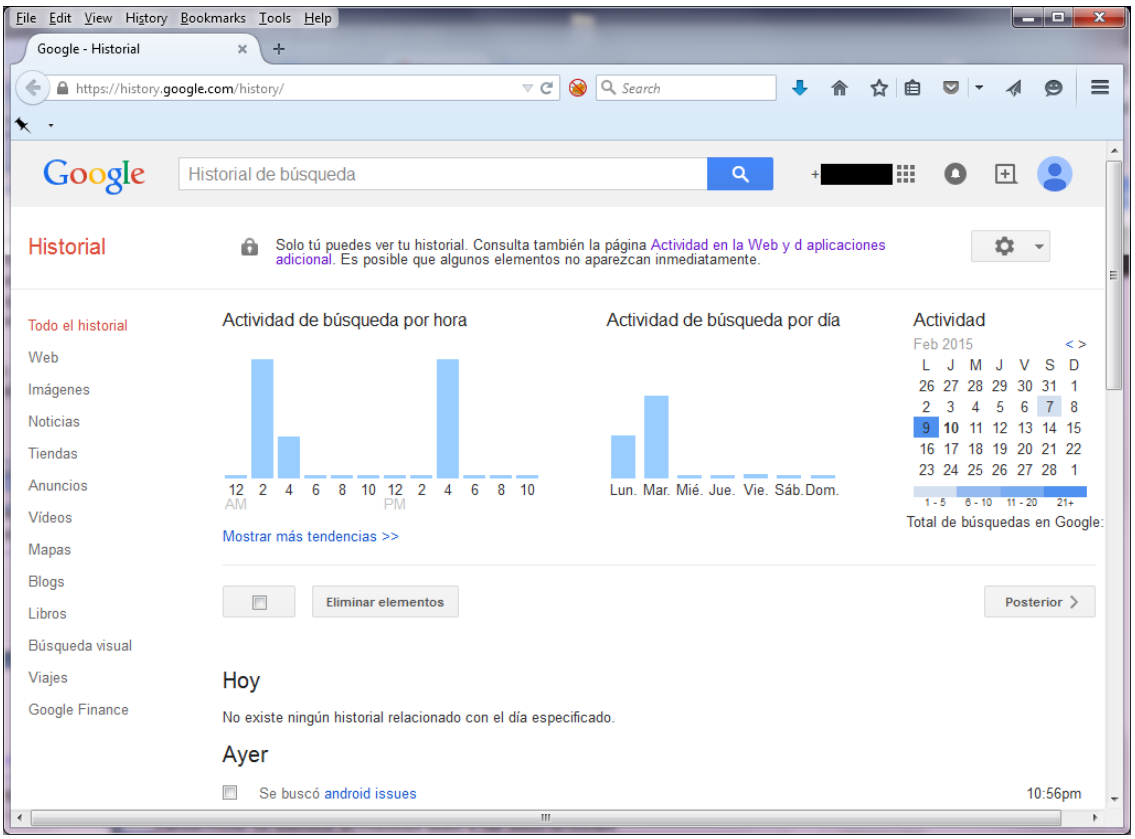
1200. Supuestamente, esta información es utilizada para proporcionarle al usuario mejores resultados y recomendaciones (más relevantes) al usar los productos y servicios de Google, como por ejemplo los servicios de búsqueda web y de mapas (con predicciones de búsqueda más precisas), conocer los resultados de las búsquedas en los que el usuario pulsa, conocer los anuncios visualizados por el usuario, poder acceder rápidamente a páginas web que ya se han visitado (disponiendo del historial de búsquedas recientes realizadas en cualquier dispositivo móvil u ordenador con la misma cuenta de usuario), la dirección IP del usuario, el tipo de navegador web empleado y su idioma, etc [Ref.- 172].

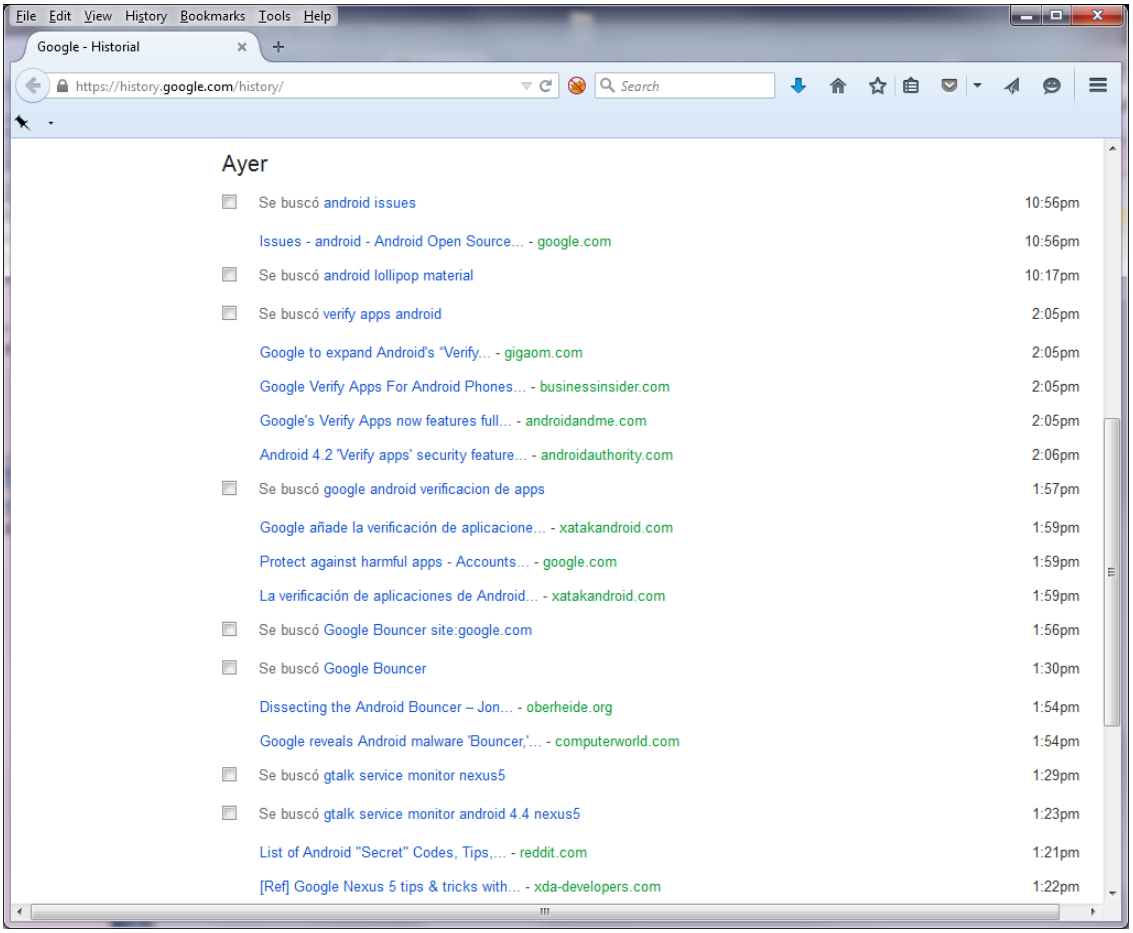
1201. El historial de actividad web y de aplicaciones puede estar desactivado si la cuenta de usuario de Google no ha sido vinculada a ningún dispositivo móvil Android, pero en caso de haberse llevado a cabo esta vinculación, y dado que esta funcionalidad está habilitada por defecto, el servicio estará activo.

1202. Si se activa desde la página web es posible especificar si se desea incluir en el historial la actividad de Chrome y de otras aplicaciones, qué estará disponible en la página "Actividad web y de aplicaciones adicional", a través de la siguiente URL: "https://history.google.com/history/app".

1203. Se recomienda no activar la funcionalidad de historial de actividad web y de aplicaciones, incluyendo estas capacidades adicionales que permiten incluir en el historial la actividad de Chrome y de otras aplicaciones, salvo que se desee hacer un uso explícito de las mismas.

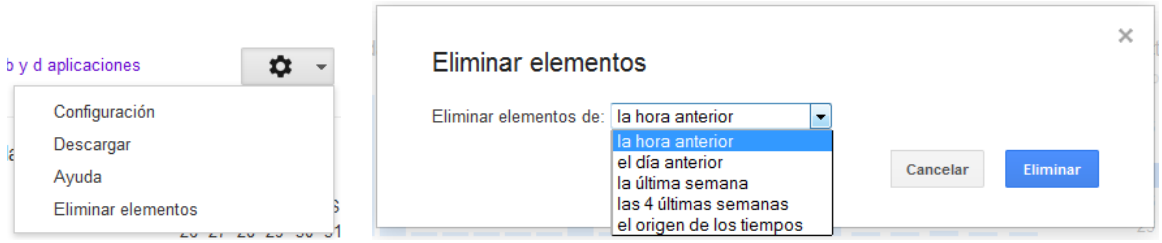
1204. La página "Actividad web y de aplicaciones" permite acceder y administrar el historial de actividad web y de aplicaciones, y dispone de detalles sobre las búsquedas y otras actividades clasificadas por servicios de Google (desde el menú de la parte izquierda: Web, Imágenes, Noticias, etc), e incluso clasificadas por fechas y horas, y obtener información detallada de todas las búsquedas realizadas:



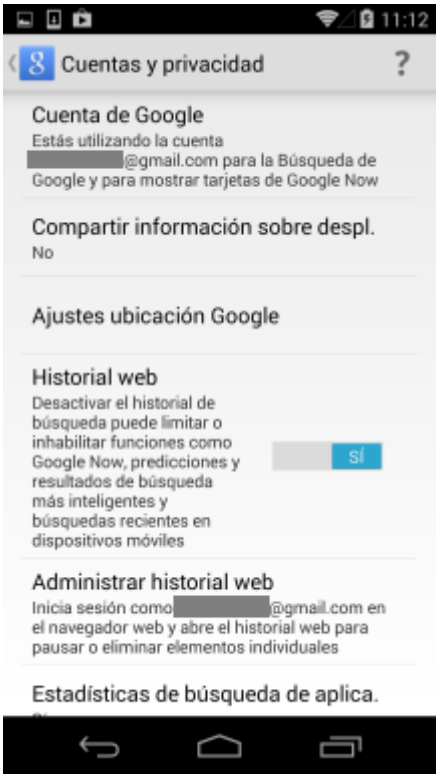


1205. Desde la página web es posible eliminar los registros del historial individualmente, o todo el historial, a través de su selección y del botón "Eliminar elementos" [Ref.- 173].

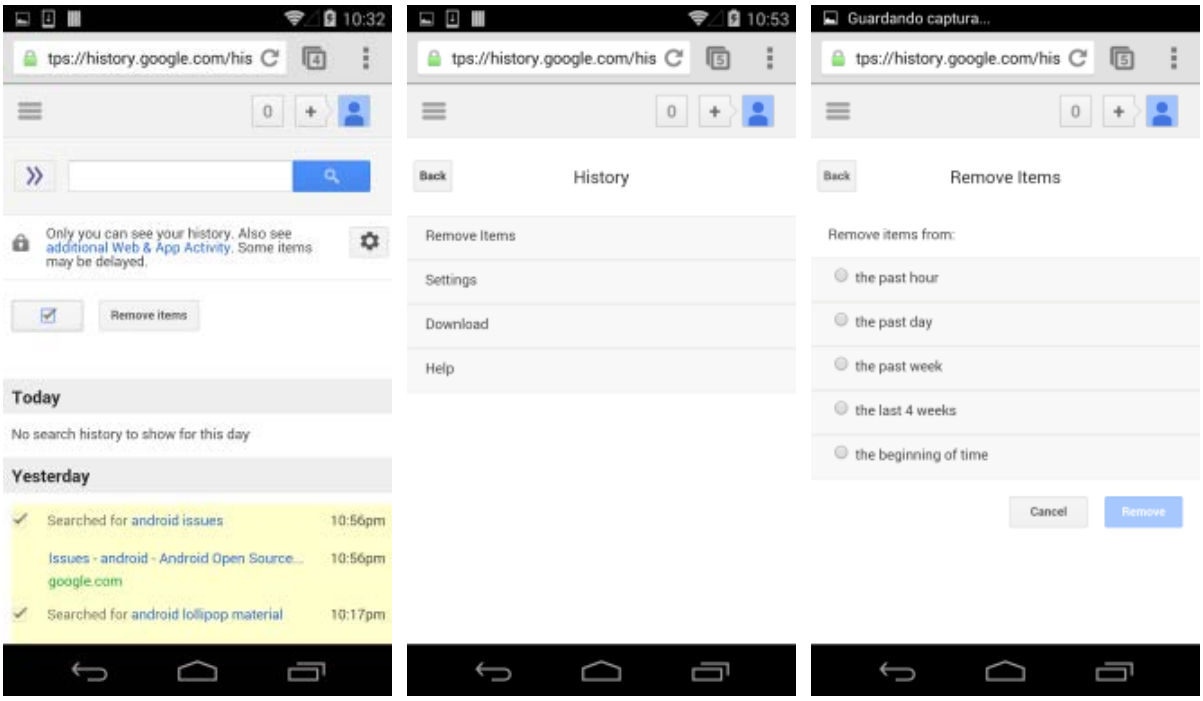
1206. Adicionalmente, desde la página web, y mediante el botón de ajustes, es posible eliminar elementos selectivamente en función del periodo temporal:



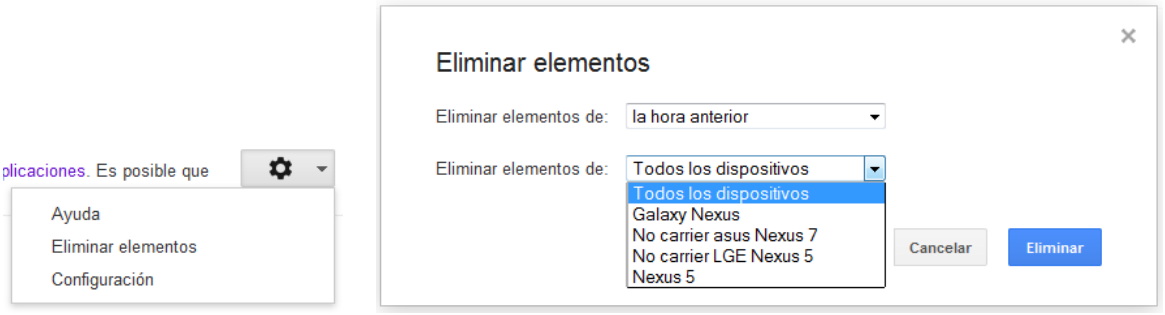
1207. El historial web puede ser desactivado en cualquier momento desde la página web y desde Android, y en concreto desde la app "Ajustes de Google" y el menú "Búsqueda y Google Now", mediante el menú "Cuentas y privacidad" y la opción "Historial web" y el botón "[SI | NO]":



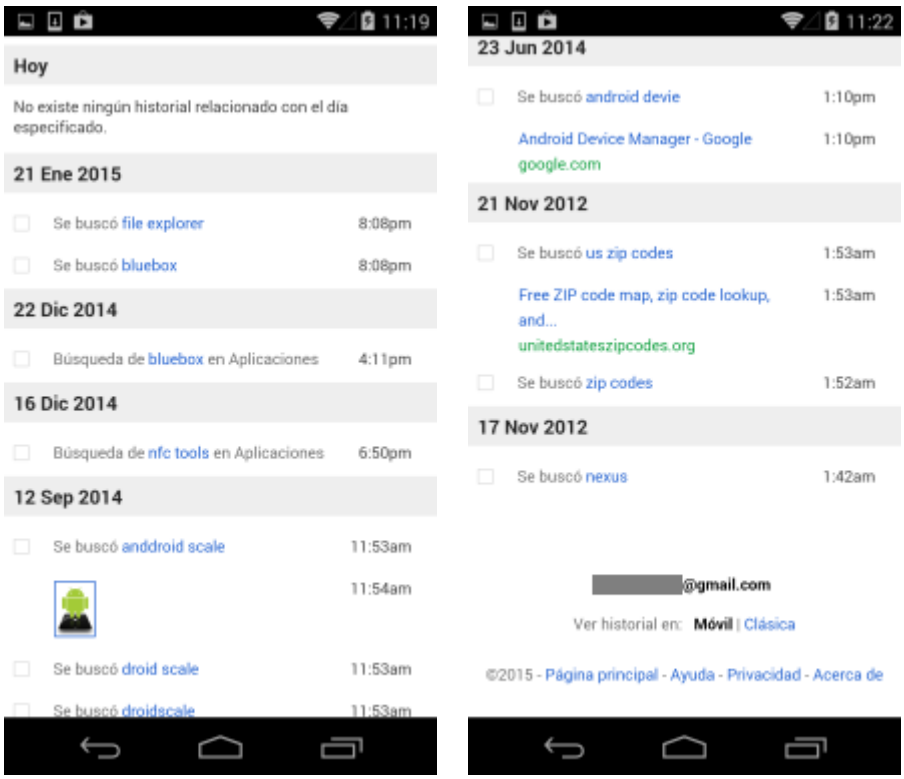
1208. Adicionalmente, se dispone de capacidades de administración del historial web desde Android mediante la opción "Administrar historial web", que abre el navegador web con una sesión asociada a la cuenta del usuario de Google empleando la URL "https://history.google.com/history/edit" (descrita previamente). Desde ésta (ya que hace uso de la misma página web) es igualmente posible eliminar elementos del historial web selectivamente, el historial al completo, o en función del periodo temporal. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:



1209. En el caso de haber incluido en el historial la actividad de Chrome y de otras aplicaciones, qué estará disponible en la página "Actividad web y de aplicaciones adicional" (descrita previamente), mediante el botón de ajustes, es también posible eliminar elementos selectivamente en función del periodo temporal, pero adicionalmente, únicamente de un dispositivo móvil específico:



1210. Los elementos del historial web incluyen términos de búsqueda, tanto en el buscador web general de Google como por ejemplo en las búsquedas por apps en Google Play, incluyendo el día y hora en que se utilizaron dichos términos, durante los últimos años:



1211. En resumen, desde el punto de vista de seguridad, y de la privacidad el usuario, no se recomienda hacer uso del historial de actividad web y de aplicaciones. Adicionalmente, se recomienda borrar el historial de actividad web y de aplicaciones actualmente existente en la cuenta de usuario de Google.

5.22.1.6 CERTIFICATE PINNING

1212. Android, desde la versión 4.2, dispone de capacidades adicionales para el uso de mecanismos de validación y protección de las comunicaciones autentificadas y cifradas mediante HTTPS (TLS), basadas en *certificate pinning* [Ref.- 76].

1213. Para ello se establece una lista de *pins*, cada uno de ellos asociado al nombre (en DNS) de un *host* o servidor específico, y se permite a nivel global del sistema que tanto el navegador web como las apps verifiquen la lista de *pins* (en caso de existir) y validen las conexiones mediante HTTPS. La lista de *pins* es almacenada en el fichero "pins" bajo "/data/misc/keychain". Por defecto el fichero "pins" no existe en Android 4.x, es decir, no se proporciona ninguna lista de *pins* por defecto:

```
- PIN list: /data/misc/keychain/pins
```

5.22.1.7 ANDROID WEBVIEWS

1214. WebView[105] es un componente empleado por las apps que permite mostrar contenidos web, como si se tratase de un navegador web personalizado, embebido y simplificado. Este contenido web puede incluir tanto páginas HTML como código JavaScript, que puede ser ejecutado por la app, por lo que las WebViews constituyen un componente crítico desde el punto de vista de seguridad en Android [Ref.- 127].

1215. Por ejemplo, mediante ataques de Cross-Site Scripting (XSS) e inyección de código JavaScript (por ejemplo en ataques MitM, Man-in-the-Middle, especialmente cuando no se hace uso de técnicas de cifrado del tráfico mediante HTTPS ni de una correcta y estricta verificación de los certificados digitales), es posible forzar a una app a ejecutar el código de un potencial atacante.

1216. Los componentes WebView son ampliamente utilizados por las apps para mostrar información, actuando de clientes web (en lugar de desarrollarse una app real completa), y por tanto, permiten obtener y mostrar contenidos o páginas web proporcionadas por los servidores y aplicaciones web asociados a la app.

1217. Existen dos métodos críticos asociados a los componentes WebView. Por un lado, el método "setJavaScriptEnabled()", que indica si se permite la ejecución de código JavaScript dentro de la WebView[106].

1218. Pese a que por defecto este método no está habilitado, es decir, los componentes WebView no ejecutan código JavaScript por defecto, esta funcionalidad suele ser habilitada por los desarrolladores de apps a través del método "setJavaScriptEnabled()".

1219. Por otro lado, el método "addJavascriptInterface()" proporciona elevadas capacidades al motor (y código) de JavaScript para invocar e interactuar con otros componentes y métodos (código) de Android. Por tanto, se recomienda sólo hacer uso del mismo por parte de las apps cuando se tenga plena confianza en el código HTML y JavaScript a ejecutar.

1220. Las versiones de Android 4.1 (API 16) e inferiores son vulnerables frente a la posibilidad de inyección de código JavaScript que permita la ejecución de comandos de sistema operativo, ya que se permite el uso de esta funcionalidad de manera generalizada y por defecto (CVE- 2012-6636).

1221. Durante los años 2011, 2012 y 2013 [Ref.- 63] se publicaron detalles del impacto y las vulnerabilidades asociadas al método "addJavascriptInterface()" de WebView en dispositivos Android <= 4.1 (API <= 16), incluyendo la posibilidad de ejecución remota de código (RCE, *Remote Code Execution*). Un potencial código JavaScript malicioso puede

[105] http://developer.android.com/reference/android/webkit/WebView.html
[106] http://developer.android.com/reference/android/webkit/WebSettings.html

hacer uso de las capacidades de interacción entre JavaScript y Java (reflexión, Java Reflection APIs), y al ser procesado por un componente WebView, ejecutar comandos de sistema operativo y código nativo a través de una shell (mediante el método "exec()" de Java y la invocación de, por ejemplo, "/system/bin/sh").

1222. Esta vulnerabilidad no sólo afectaba a los componentes WebView de las apps de terceros de Android, sino también a apps nativas como el navegador web existente por defecto, por ejemplo en Android 4.1.2, al disponer del método "addJavascriptInterface()" habilitado por defecto (CVE-2013-4710) [Ref.- 149], o incluso en Android 4.2 y 4.3 (Jelly Bean) (CVE-2014-1939)[107].

1223. La criticidad de esta vulnerabilidad es muy elevada, debido al número de componentes y apps que pueden verse afectados, y a la existencia de exploits disponibles públicamente (por ejemplo, en entornos ofensivos como Metasploit[108]).

1224. Versiones posteriores de Android, como Android 4.2 o superiores, también pueden ser vulnerables si las apps hacen uso de WebView y del método "addJavascriptInterface()" con compatibilidad para versiones anteriores de Android (4.1 o previas), o si por ejemplo, las apps emplean librerías de servicios y redes de publicidad y anuncios (Ads) que hacen uso de estas mismas capacidades dentro de la app. El impacto de un potencial ataque depende de los permisos y capacidades de cada app.

1225. Por defecto, desde la versión 4.2 de Android (API 17), y en concreto en el caso de las apps específicamente compiladas para esa versión (y/o versiones superiores) de Android (mediante la directiva "targetSdkVersion"), la vulnerabilidad ha sido mitigada. Para evitar este tipo de ataques, los componentes WebView, aunque dispongan del método "addJavascriptInterface()" habilitado, deben declarar específicamente la anotación "@JavascriptInterface"[109] para cada método que desean pueda ser invocado desde código JavaScript, y además esos métodos deben ser declarados como públicos.

1226. La implementación de WebView en Android estaba basada en WebKit[110] (motor utilizado por el navegador web por defecto de Android, Android Browser) hasta la versión Android 4.4, dónde se empezó a hacer uso por defecto de Chromium[111] (motor utilizado por el nuevo navegador web existente por defecto en Android 4.4 o posterior, Chrome).

1227. Numerosas otras vulnerabilidades de seguridad que afectan a los componentes WebView han sido descubiertas y publicadas en los últimos años, afectando a versiones de Android inferiores a 4.4 (KitKat) [Ref.- 149] [Ref.- 62], tanto en su integración con JavaScript, como facilitando la utilización de técnicas de ataque para evitar la aplicación de la Same Origin Policy (SOP) en WebViews o el navegador web [Ref.- 115] [Ref.- 97], habiéndose publicado numerosas vulnerabilidades sobre la SOP (también conocidas como UXSS, Universal Cross-Site Scripting) para Android 4.3 [Ref.- 62].

1228. Google confirmó en enero de 2015 que no proporcionará actualizaciones y parches de seguridad para WebView en versiones de Android previas a 4.4 [Ref.- 116].

1229. Por tanto, se recomienda actualizar a la versión 4.4 de Android (KitKat), o en su defecto, hacer uso de navegadores web que disponen de su propio motor de renderización

[107] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1939
[108] http://www.rapid7.com/db/modules/exploit/android/browser/webview_addjavascriptinterface
[109] http://developer.android.com/guide/webapps/webview.html
[110] https://www.webkit.org
[111] http://www.chromium.org

(capacidad de procesar y mostrar contenidos web), como por ejemplo Chrome (disponible para Android 4.0 o superior) o Firefox (disponible para Android 2.3 o superior) para Android.

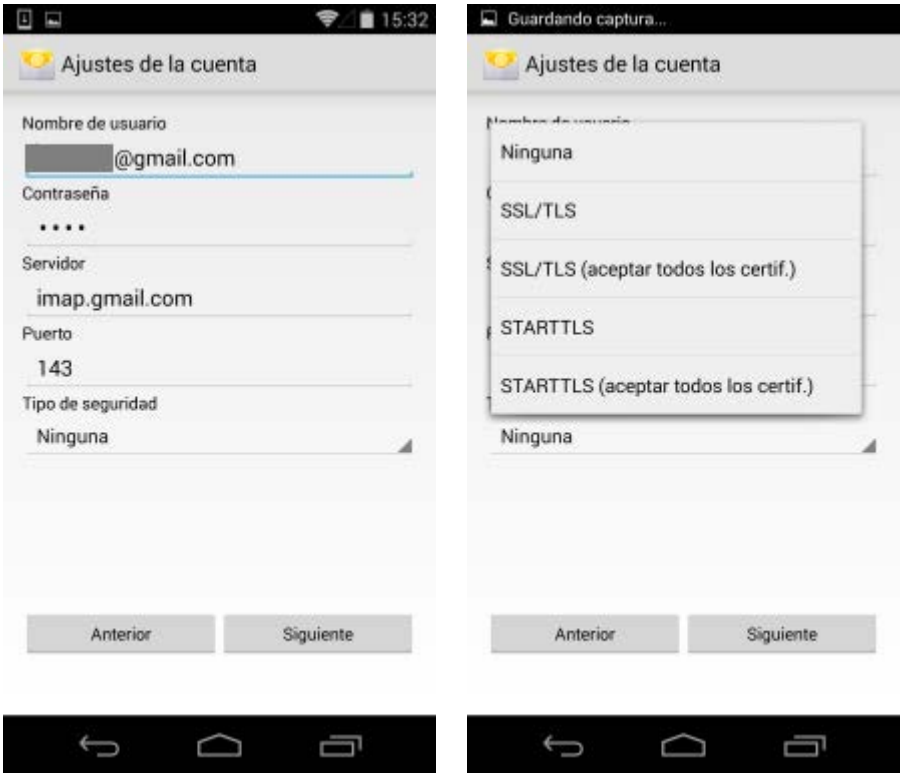
5.22.2 CORREO ELECTRÓNICO (E-MAIL) Y GMAIL

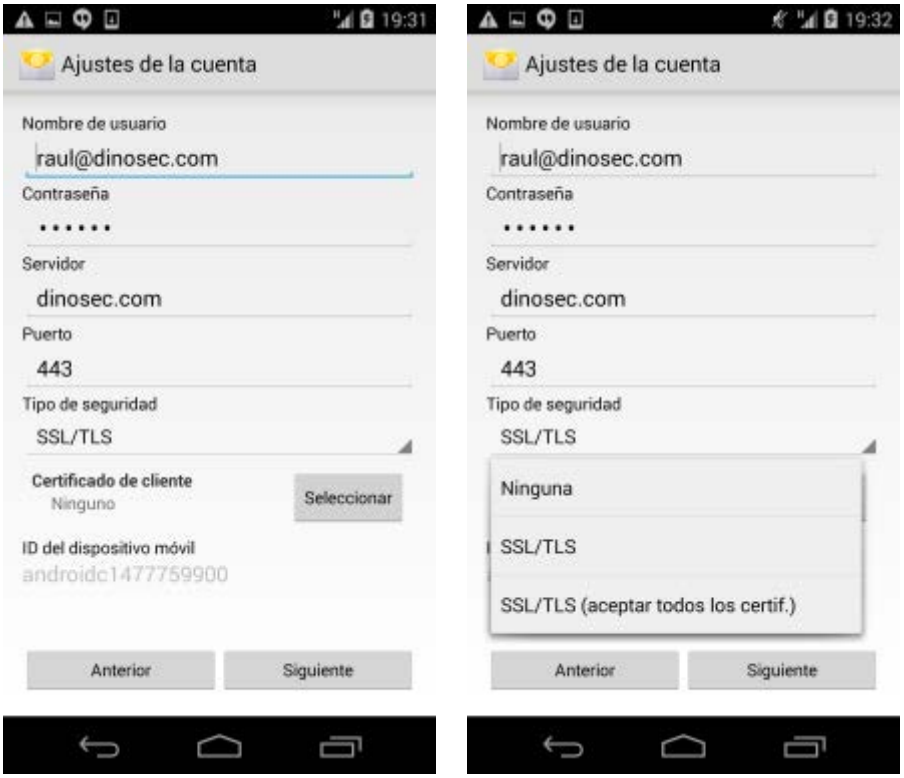
1230. Android proporciona múltiples capacidades para la gestión de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través del icono o app "Correo" (app genérica de correo) desde el *Launcher* (como por ejemplo cuentas de correo de Exchange, IMAP o POP3, cuyo análisis detallado queda fuera del alcance de la presente guía), o desde el icono o app de "Gmail" (app específica de acceso a Gmail), dónde es posible configurar una o varias cuentas de correo electrónico (en ambos casos).

1231. Asimismo, existe una relación muy estrecha entre las cuentas de correo electrónico registradas, y las cuentas vinculadas al dispositivo móvil (ver apartado "5.18. Cuenta de usuario de Google").

1232. Si se lleva a cabo la configuración de cuentas de correo electrónico mediante Exchange, POP3, o IMAP, incluyendo el envío de e-mails mediante SMTP, se recomienda siempre habilitar la opción de seguridad para hacer uso de conexiones cifradas (TLS), y deshabilitar cualquier opción que permita aceptar todos los certificados TLS (como aquellos no válidos o autofirmados).

1233. La opción de tipo de seguridad disponible por defecto para IMAP y POP3 al añadir una nueva cuenta de correo electrónico es "Ninguna":





1234. En el caso de Exchange, la opción por defecto es "SSL/TLS", disponiéndose adicionalmente de la posibilidad de seleccionar un certificado digital cliente de usuario para llevar a cabo la autentificación con el servidor de correo electrónico.

1235. En cualquier caso, debe siempre seleccionarse "SSL/TLS" o "STARTTLS", haciendo énfasis en qué en ningún caso debe seleccionarse ninguna de las opciones con el texto "(aceptar todos los certificados)".

1236. Debido a que la vinculación del dispositivo móvil con una cuenta de usuario de Google es prácticamente obligatoria, y a la relación existente entre esta cuenta y el servicio de correo de Google, Gmail, esta funcionalidad estará habilitada normalmente.

1237. Desde el punto de vista de seguridad, no se disponen de opciones avanzadas de configuración asociadas a Gmail desde el dispositivo móvil Android, ni siquiera a través del menú "Ajustes", haciendo por defecto uso de cifrado mediante TLS.

1238. Adicionalmente, el acceso a los servicios de Google desde Android, y en concreto desde la versión 4.4 de Android, por ejemplo a Gmail, YouTube o Google Play (entre otros), hace uso de mecanismos de protección propios basados en *certificate pinning*[112], no aceptándose cualquier certificado digital como válido al establecerse una conexión cifrada mediante TLS con los servidores de Google [Ref.- 76].

1239. Respecto a la gestión de las credenciales de acceso a Gmail, se recomienda seguir las recomendaciones descritas en el apartado "5.18. Cuenta de usuario de Google".

1240. Por defecto, al escribir un nuevo mensaje o e-mail desde la app de Gmail, el dispositivo móvil no añade ninguna firma, opción recomendada desde el punto de vista de seguridad para evitar indicar desde dónde se realiza el envío, como por ejemplo "Enviado desde un dispositivo móvil":

[112] https://developer.android.com/training/articles/security-ssl.html

1241. Se recomienda mantener la configuración por defecto, sin firma, para no revelar información del fabricante o tipo de dispositivo móvil. En caso de querer añadir una firma, en ningún caso debería incluir detalles del terminal.

1242. La gestión de las firmas se puede realizar desde el botón de menú de la app de Gmail, mediante la opción "Ajustes - <cuenta de usuario de Google> - Firma" (por defecto "Sin configurar").

5.22.3 REDES SOCIALES

1243. Android 4.x no incluye por defecto apps para el acceso a diferentes redes sociales disponibles en Internet, qué si estaban incluidas en versiones previas de Android (2.x). La existencia de estas apps por defecto es siempre dependiente del fabricante u operador de telefonía móvil que comercializa el dispositivo móvil, como por ejemplo Facebook o Twitter para Android.

Nota: otros dispositivos móviles basados en Android, así como otras versiones de Android, incluyen adicionalmente apps de acceso a otras redes sociales y servicios Web 2.0.

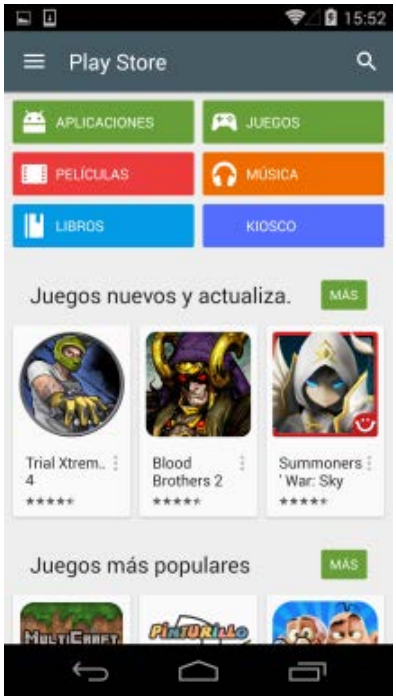
1244. En el caso de Android 4.x sólo se dispone de acceso a las apps para las redes sociales propias de Google, como por ejemplo YouTube y Google+.

1245. Siempre se recomienda antes de hacer uso de cualquiera de las apps disponibles por defecto en el dispositivo móvil, o instaladas posteriormente, realizar un análisis de seguridad en profundidad para identificar posibles comportamientos vulnerables.

5.22.4 APPS DE TERCEROS: GOOGLE PLAY

1246. Google Play (anteriormente denominado Android Market), es empleado por Google para la distribución y venta de apps y software para la plataforma Android, es decir, constituye el mercado oficial de aplicaciones móviles (apps) de Google.

1247. Android incluye una app, denominada "Play Store", disponible desde el *Launcher*, para el acceso a este servicio directamente desde el dispositivo móvil:



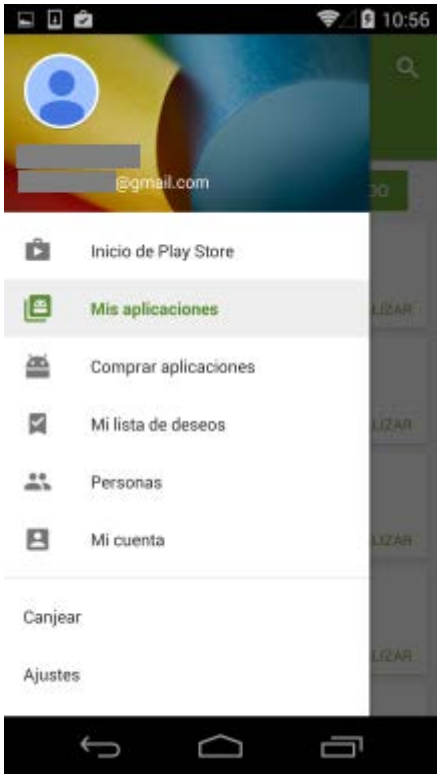
1248. La primera vez que se utiliza Play, la app solicita al usuario disponer de una cuenta de usuario de Google (si no se ha configurado una todavía en el dispositivo móvil), y le permite darla de alta o crear una nueva (ver apartado "5.18. Cuenta de usuario de Google"), tras aceptar los términos del servicio.

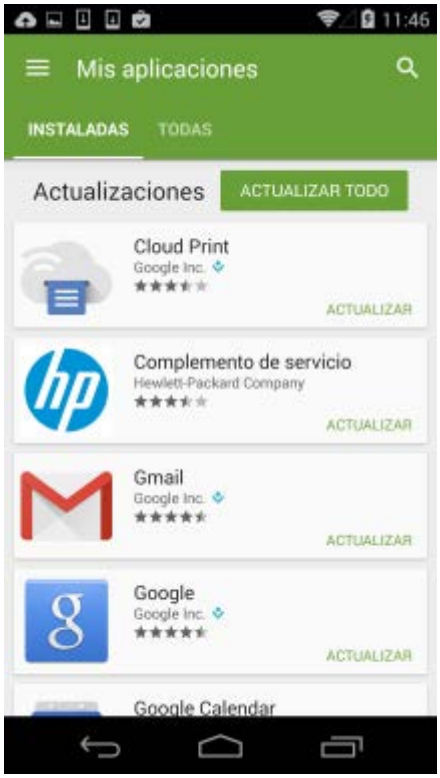
1249. La conexión de autentificación empleando la cuenta de usuario de Google, y el acceso a Google Play, se realiza a través de HTTPS hacia los servidores "www.google.com", "android.clients.google.com", "*.googleusercontent.com", y hacia otros servicios de Google.

1250. Teóricamente, la integridad de las apps de Android se verifica a través de una firma digital asociada al fichero binario (.apk) descargado, pero una posible ausencia de cifrado en el tráfico empleado para descargar las apps (mediante HTTP), no así en el tráfico de acceso a Google Play que emplea HTTPS, abre potencialmente la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de apps válidas firmadas digitalmente.

1251. Se recomienda actualizar a la última versión de las apps ya instaladas en el dispositivo móvil (ver apartado "5.22.5. Actualización de apps en Android"), ya que éstas proporcionarán posibles soluciones frente a vulnerabilidades de seguridad públicamente conocidas.

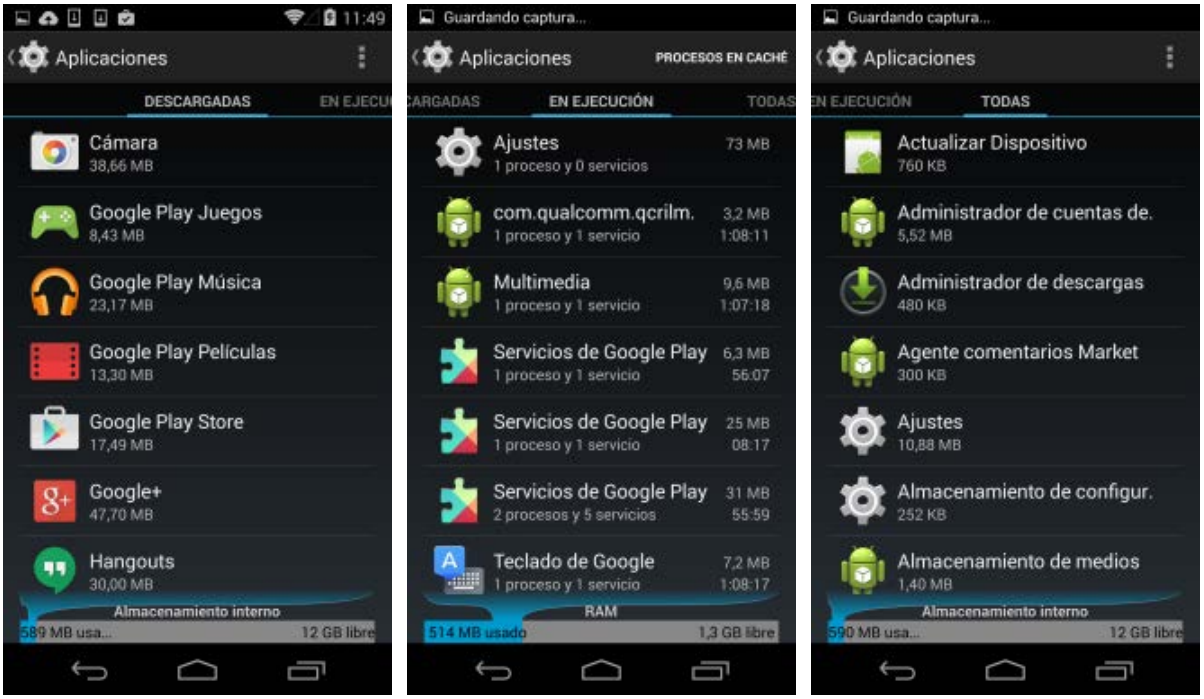
1252. La lista de programas o apps instaladas desde Google Play es accesible desde la propia app "Play Store", mediante el icono de menú es posible acceder a la sección "Mis aplicaciones" de Google Play, disponiéndose de dos pestañas para clasificar las apps instaladas en el dispositivo móvil ("Instaladas"), y todas las apps asociadas a la cuenta de usuario de Google ("Todas"):



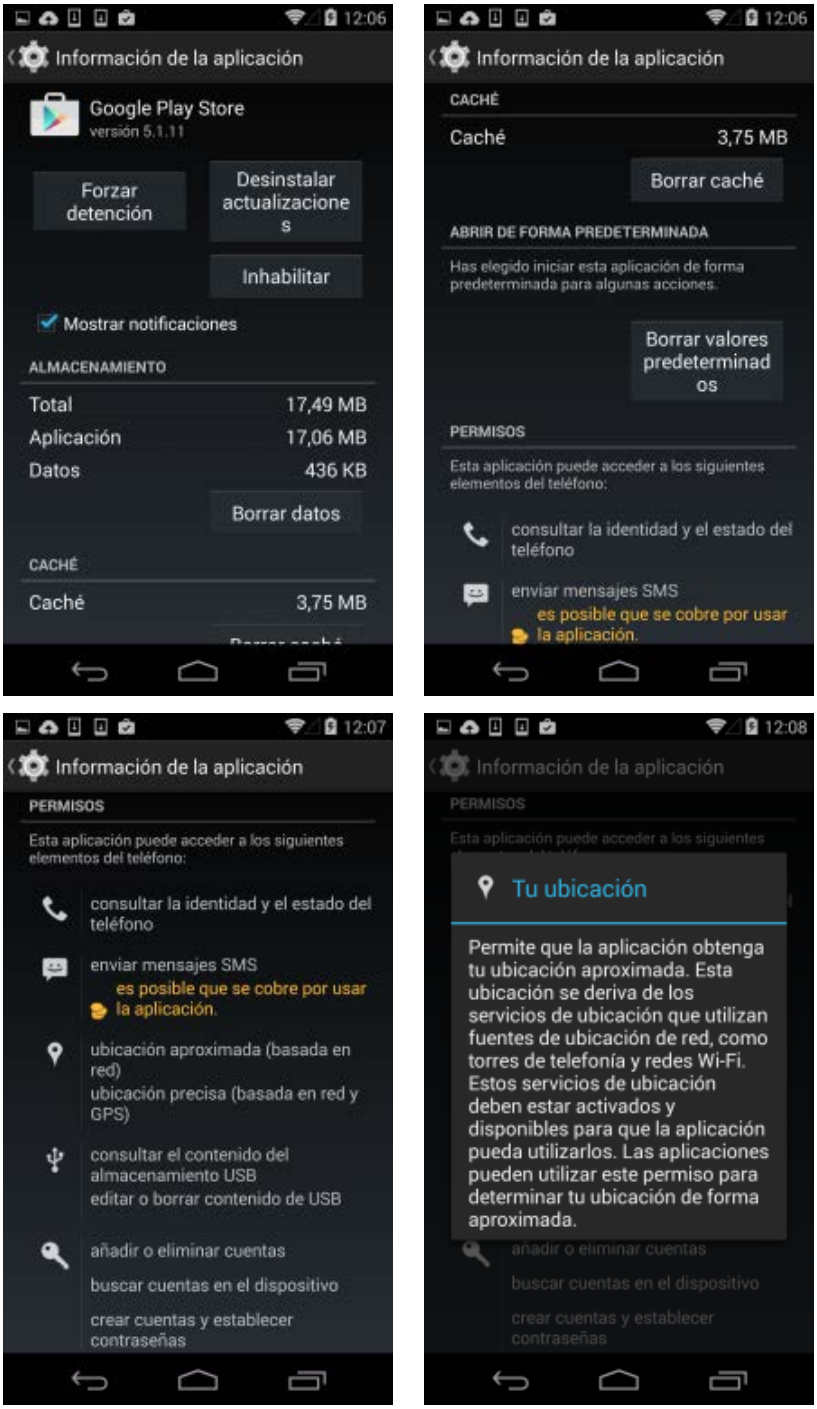


1253. Desde la app "Play Store" es posible, una vez se ha seleccionado una app, ver todos sus detalles (al igual que desde la web de Google Play), como por ejemplo su descripción, las novedades, el número de descargas, las valoraciones y comentarios de otros usuarios (siendo posible emitir una valoración), las categorías o tipo de app, enlaces a apps similares, la clasificación de su contenido, la versión y fecha de la última actualización, el tamaño, la información de contacto del desarrollador, su política de privacidad, u obtener información sobre los permisos solicitados por la app, entre otros. Adicionalmente, es posible abrirla, actualizarla, e instalarla (si todavía no está disponible en el dispositivo móvil):

1254. Adicionalmente, el listado de apps está disponible también desde el propio Android a través del menú "Ajustes [Dispositivo] - Aplicaciones", seleccionando las pestañas "Descargadas", "En Ejecución", o "Todas", para clasificar las apps que han sido instaladas alguna vez en el dispositivo móvil, que están ejecutando actualmente, o todas las apps:



1255. Desde el menú "Ajustes [Dispositivo] - Aplicaciones" es posible, una vez se ha seleccionado una app, ver todos sus detalles técnicos como por ejemplo la versión, el tamaño (total, y dividido por la app y por sus datos), el tamaño ocupado en caché, determinar si se mostrarán notificaciones generadas por la app, u obtener información sobre los permisos solicitados por la app, entre otros. Mediante la selección de cualquier permiso es posible obtener una descripción general del mismo. Adicionalmente, es posible forzar la detención de la app si no responde, desinstalar actualizaciones (instaladas previamente para dicha app, es decir, permitiendo la sustitución de la app por su versión de fábrica), inhabilitarla, borrar sus datos o su caché, y borrar los valores predeterminados, que indican para qué acciones se iniciará esta app:



Nota: los desarrolladores interesados en la creación de apps para Android disponen de todos los detalles e información en el portal para desarrolladores *Google Play Developer Console* (https://play.google.com/apps/publish) [Ref.- 7].

1256. Debe tenerse en cuenta que la disponibilidad de una app en Google Play no asegura que la misma no sea maliciosa y pueda llevar a cabo acciones desde el dispositivo móvil dónde ha sido instalada que afecten a la seguridad y privacidad del usuario [Ref.- 1].

1257. Se recomienda analizar en detalle el contenido y procedencia de una app de terceros antes de instalarla desde Google Play en el dispositivo móvil, por ejemplo, identificando a su desarrollador, el tiempo que lleva la app publicada en Google Play, su valoración y reputación por parte de otros usuarios, etc.

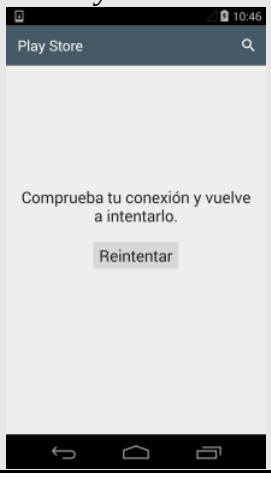
1258. Una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil y ambos han sido vinculados (ver apartado "5.18. Cuenta de usuario de Google"), también desde la sección de "Ajustes" de la aplicación web de Google Play ("https://play.google.com/store/account") es posible gestionar las apps disponibles (ver apartado "5.23. Instalación y eliminación de apps en Android") y, a través del "Administrador de dispositivos Android" (ver apartado "5.3. Gestión empresarial de dispositivos móviles basados en Android"), el o los dispositivos móviles asociados a la cuenta del usuario.

5.22.5 ACTUALIZACIÓN DE APPS EN ANDROID

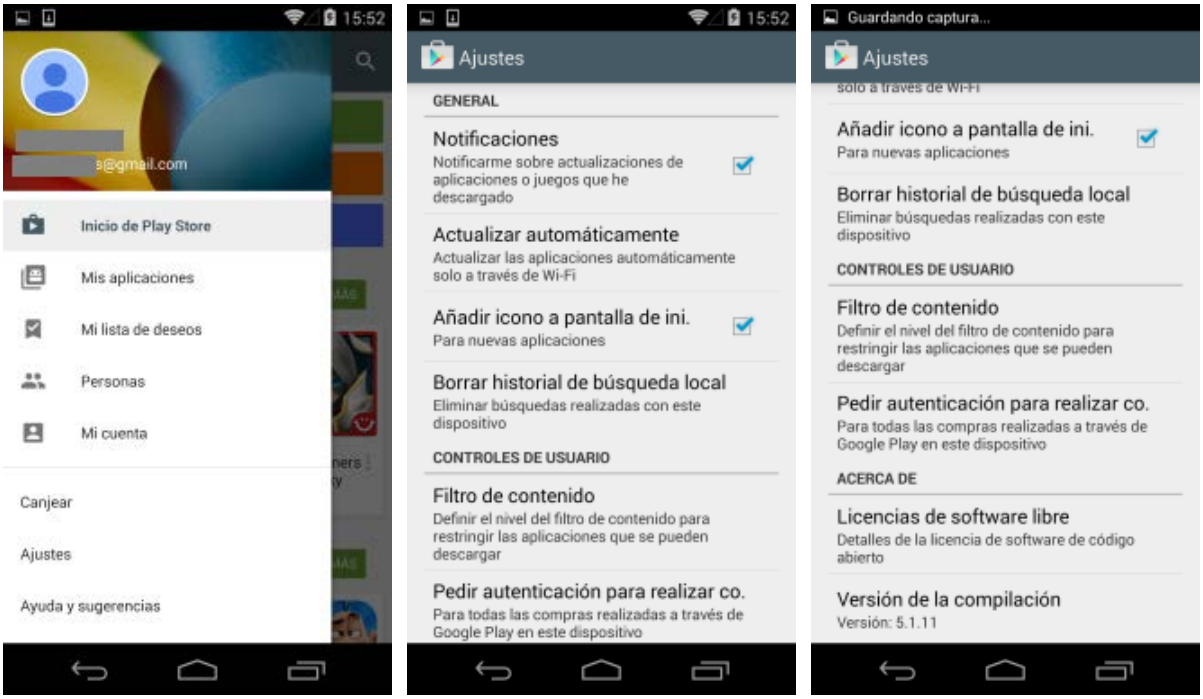
1259. El término apps o aplicaciones móviles engloba en el presente apartado al conjunto de aplicaciones móviles de sistema o de terceros que son compatibles con Android y que pueden ser instaladas sobre este sistema operativo.

Nota: pese a que Android permite la instalación de apps de terceros desde fuentes no oficiales (ver apartado "5.23. Instalación y eliminación de apps en Android"), el análisis de las actualizaciones de apps en Android se centra en las aplicaciones móviles disponibles a través del mercado oficial de Google, Google Play.

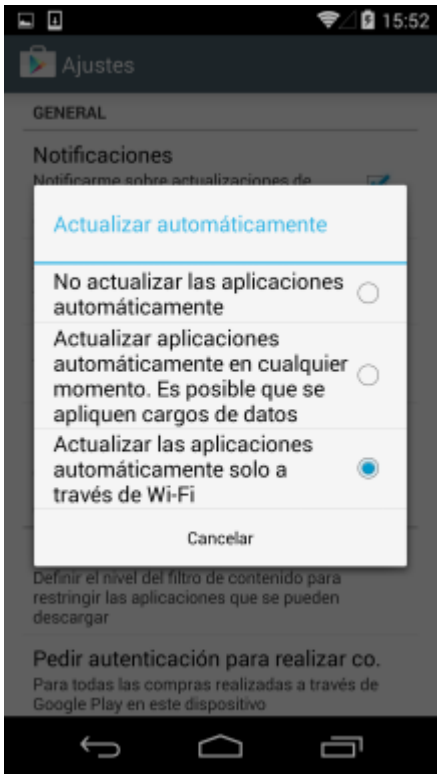
La app "Play Store" no puede ser ejecutada si no se dispone de conectividad de datos (autentificada y cifrada) hacia Google Play en Internet (Wi-Fi o 2/3/4G), mostrándose el siguiente mensaje: "*Comprueba tu conexión y vuelve a intentarlo. [Reintentar]*":



1260. Desde la app de Google Play, denominada "Play Store", y mediante el icono de menú es posible acceder a la sección de "Ajustes". En el apartado "General" es posible configurar como se desea que se produzca el proceso de actualización de las apps instaladas desde Google Play mediante la opción "Actualizar automáticamente". Se dispone de la opción de que no se actualicen las apps automáticamente, que se actualicen las apps automáticamente en cualquier momento, o sólo a través de redes Wi-Fi:



1261. En caso de estar interesados en actualizar las apps tan pronto estén disponibles, tanto a través de redes Wi-Fi como de redes de datos móviles 2/3/4G, se recomienda no activar la opción "Actualizar las aplicaciones automáticamente solo a través de Wi-Fi" (habilitada por defecto):



1262. En Android 4.4, el acceso a Google Play (incluyendo el proceso de verificación de actualizaciones de las apps) se realiza a través de una comunicación HTTPS cifrada empleando mecanismos de protección propios basados en *certificate pinning*, no aceptándose cualquier certificado digital como válido al establecerse una conexión cifrada mediante TLS con los servidores de Google Play [Ref.- 76].

1263. Sin embargo, algunas conexiones no hacen uso de estos mecanismos y permiten identificar fácilmente[113] que la descarga de la actualización se intenta realizar desde el servidor "android.clients.google.com", mediante HTTPS. La respuesta redirige a la app "Play Store" hacia los servidores bajo el dominio "*.gvt1.com", también empleando HTTPS, para que ésta lleve a cabo una segunda petición solicitando el binario correspondiente a la app a actualizar:

1264. El proceso de descarga e instalación de una nueva actualización solicita el paquete o app a descargar y desvela numerosos detalles del dispositivo móvil y del software involucrado, como números de versiones, identificadores, cookies, agente de usuario, etc:

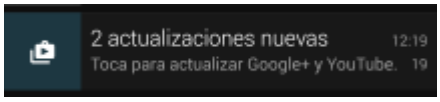
```
GET
/market/download/Download?packageName=com.google.android.apps.cloudprint&
versionCode=92&ssl=1&token=...UxPvc&downloadId=4622851621093408308&gz=1
HTTP/1.1
User-Agent: AndroidDownloadManager/4.4.4 (Linux; U; Android 4.4.4; Nexus
5 Build/KTU84P)
Cookie: MarketDA=17368976975591456789
Host: android.clients.google.com

--

GET
/market/GetBinary/GetBinary/com.google.android.apps.cloudprint/92/apk_gz?
mm=31&ms=au&mt=1424284512&mv=m&nh=EAE&pl=22&expire=1424457364&ipbits=0&ip
=0.0.0.0&cp=SmFwa2V1R1o6MzY1NjAxMDEwMTc0MTE2NzA3MTg&sparams=expire,ipbits
,ip,q:,cp&signature=D6D771C464C557A32E4183DAC3BC3C2503B082DE.76DB85DC02DB
556759C6E0170FA64B972D18A02C&key=am3 HTTP/1.1
```

[113] Mediante la utilización de una CA privada propia, y sin que sea necesario manipular el proceso de verificación de *certificate pinning* en el propio dispositivo móvil.

```
Host: <...>.gvt1.com
```

1265. Por otro lado, las imágenes (RIFF, "image/webp") de Google Play se obtienen mediante HTTP desde los servidores "lhX.ggpht.com", dónde "X" corresponde a un dígito.

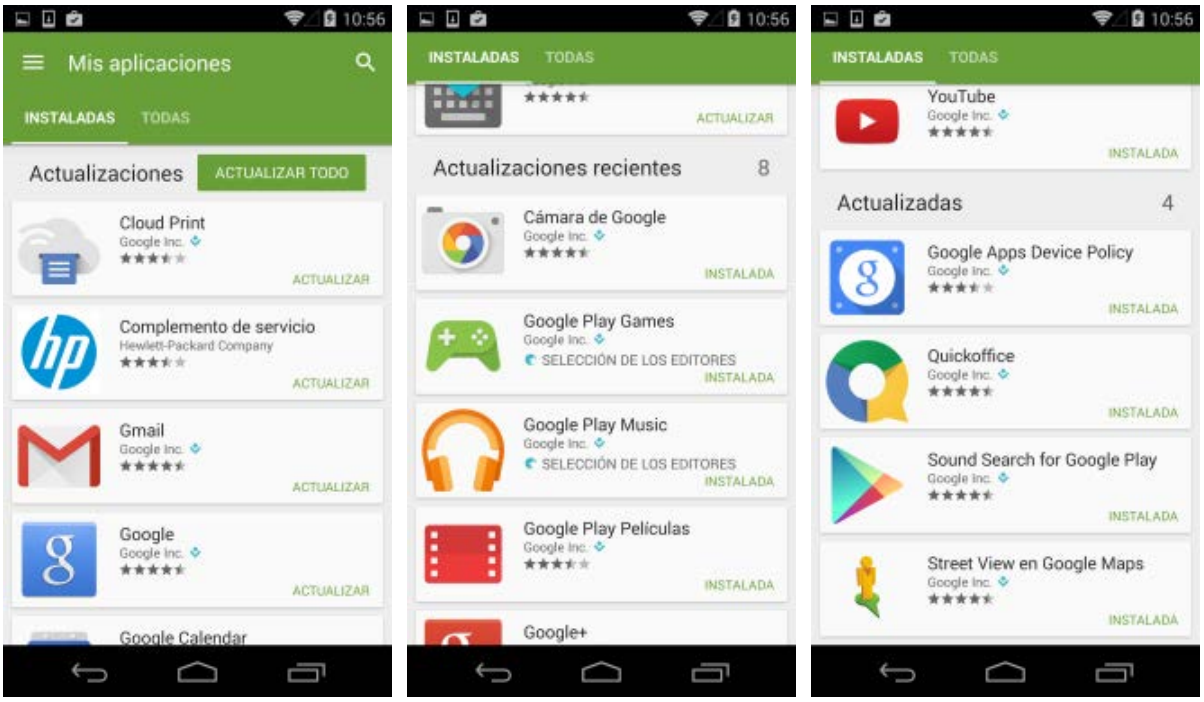
1266. Por defecto, la barra de notificaciones de Android mostrará un aviso sobre la disponibilidad de actualizaciones para las apps, en caso de no haber seleccionado la opción de actualización automática (ya que en ese caso las actualizaciones podrían ser llevadas a cabo sin la intervención del usuario, en concreto, si no solicitan nuevos permisos):



1267. Mediante la selección de dicha notificación, el usuario puede identificar para qué apps se dispone de actualización y los detalles asociados.

1268. La configuración de las notificaciones está disponible desde la app "Play Store", a través del icono de menú, de la sección de "Ajustes", y mediante la opción "Notificaciones".

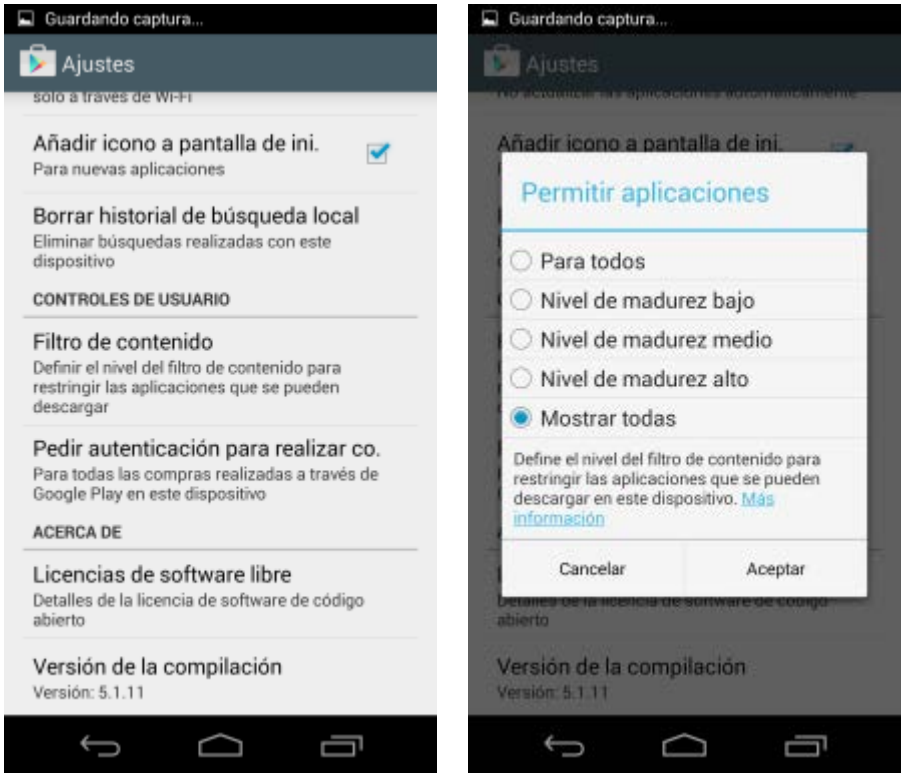
1269. La pantalla de actualizaciones está disponible desde la propia app "Play Store", mediante el icono de menú, accediendo a la sección "Mis aplicaciones" y a la pestaña con la lista de las apps instaladas en el dispositivo móvil ("Instaladas"). Esta pestaña dispone de una sección denominada "Actualizaciones", por encima de las secciones de apps instaladas y actualizadas ("Actualizaciones recientes" y "Actualizadas"):



1270. Desde la misma se proporcionan detalles sobre las actualizaciones disponibles para las apps descargadas e instaladas en el dispositivo móvil, así como del resto de apps instaladas para las que no existe actualmente una actualización.

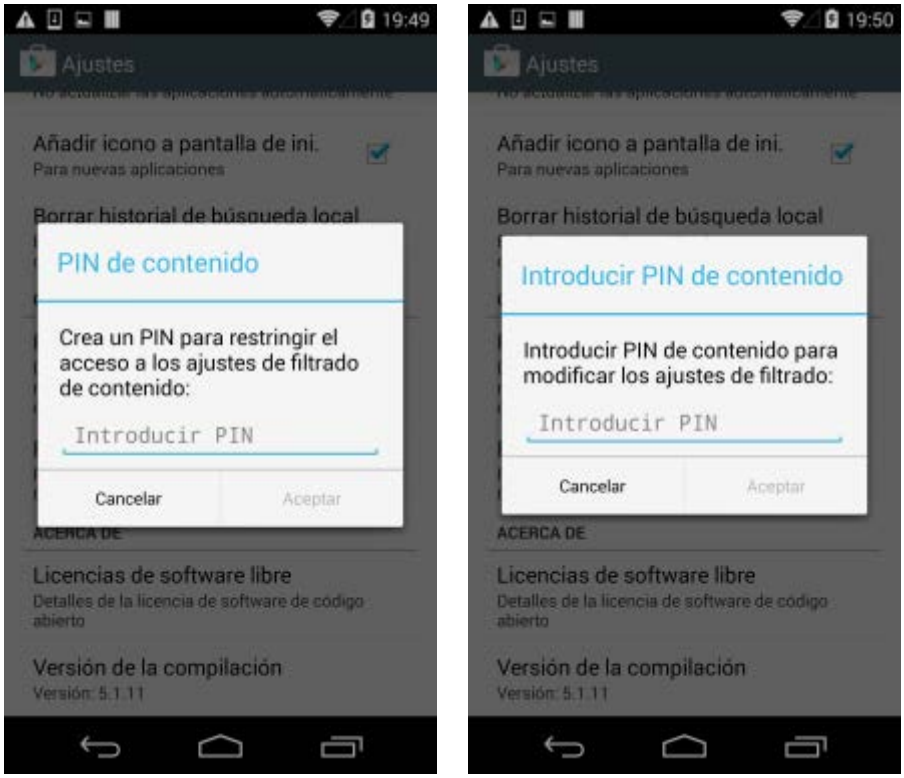
1271. Desde esta pantalla el usuario puede actualizar manualmente cada una de las apps, o todas ellas simultáneamente (botón "Actualizar Todo").

1272. Adicionalmente, Android permite a través de la opción "Filtro de contenido", disponible desde la sección "Ajustes [Controles de Usuario]" de la app "Play Store", seleccionar el nivel de filtro permitido para la instalación (y navegación por Google Play) de apps, en función de su nivel de madurez. Por defecto se muestran todas las apps:

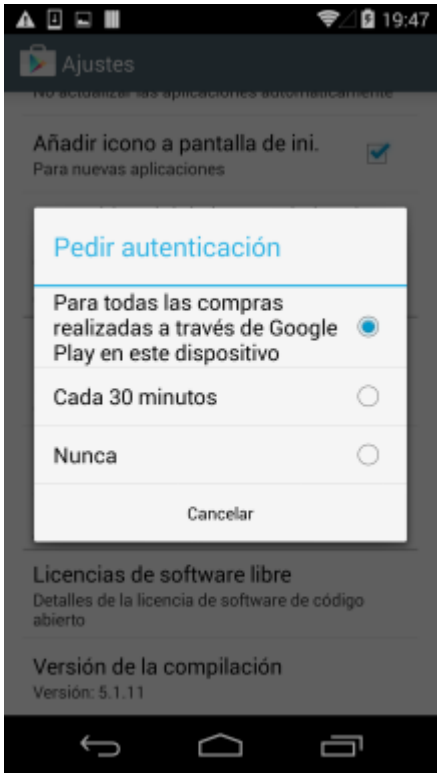


1273. El nivel de madurez se evalúa en función de los contenidos de la app (violencia – real o fantástica, referencias sexuales, contenido ofensivo, material inadecuado, etc.) y del tipo de datos del usuario recopilados por la app (ubicación, funciones sociales, compartir datos con otros usuarios, etc.) [Ref.- 104].

1274. Si se modifica el conjunto de apps a mostrar, la opción "PIN de contenido" permite al usuario establecer un PIN para evitar cambios en los controles de usuario y filtros de contenido por parte de otros usuarios del dispositivo móvil (como por ejemplo menores de edad):



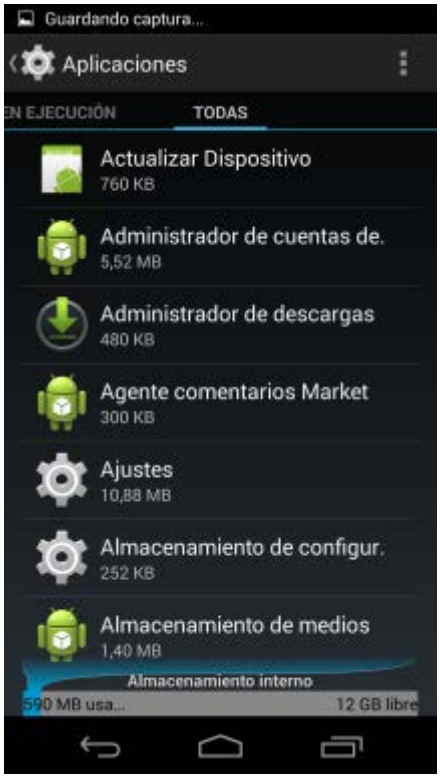
1275. Asimismo, la opción "Pedir autenticación para realizar compras" (habilitada por defecto y opción recomendada desde el punto de vista de seguridad) permite establecer controles para que a la hora de instalar una nueva app de pago desde Google Play, se solicite autorización al usuario, junto a sus credenciales:



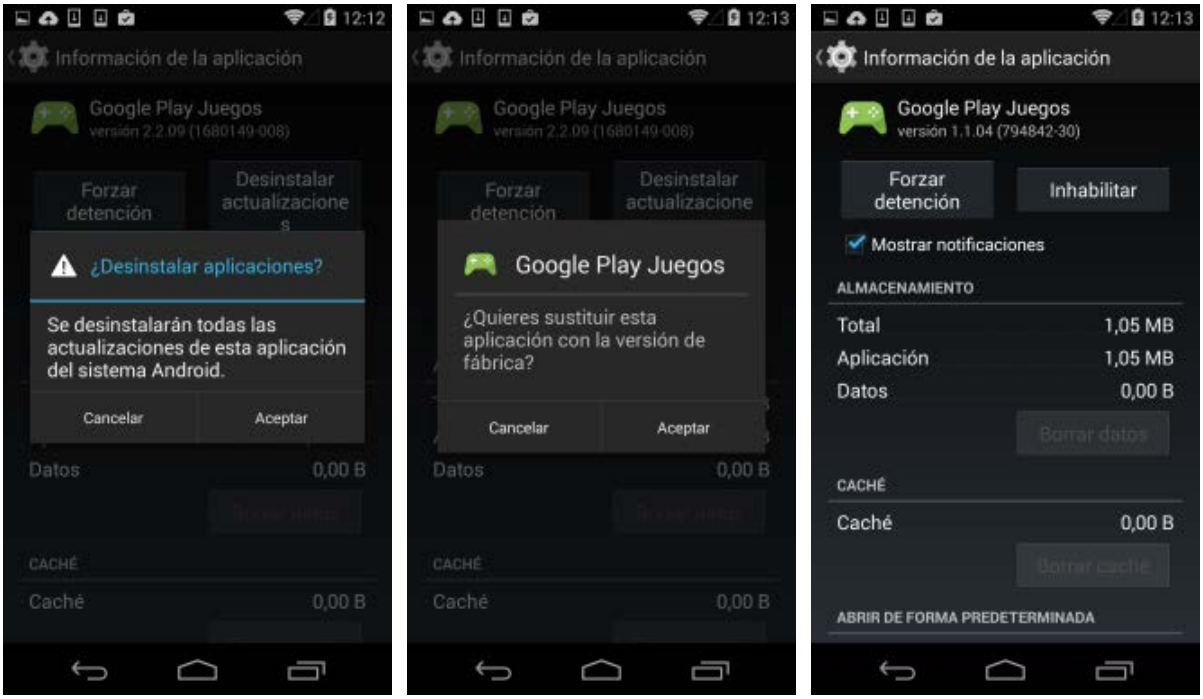
1276. Esta solicitud puede hacerse válida para los siguientes 30 minutos, con el objetivo de facilitar la realización de múltiples compras sin que sea necesario autentificarse para cada una de ellas, o nunca (opción desaconsejada).

1277. La propia app "Play Store" se actualiza automáticamente cuando hay disponibles nuevas versiones de sí misma, de forma silenciosa, sin solicitar permiso o notificar al usuario. No se dispone de ninguna opción para que esta actualización no se lleve a cabo. La actualización se lleva a cabo tras ejecutar la app "Play Store" y acceder a la pantalla principal de Google Play.

1278. La versión de la app "Play Store", al igual que de cualquier otra app instalada en Android, puede obtenerse tanto desde la propia app (menú "Ajustes [Acerca de]", como desde el menú "Ajustes [Dispositivo] - Aplicaciones", por ejemplo, desde la pestaña "Todas", seleccionando la app (en el ejemplo inferior, "(Google) Play Store") de la lista de todas las apps disponibles (por ejemplo, versión 5.1.11):



1279. La pantalla de información de la app permite tanto desinstalar la app (para aplicaciones de terceros), mediante el botón "Desinstalar", como desinstalar todas las actualizaciones disponibles (para aplicaciones nativas del sistema y disponibles por defecto en Android), mediante el botón "Desinstalar actualizaciones", ya que estas apps nativas no pueden ser desinstaladas completamente:



1280. Con el objetivo de disfrutar del mayor nivel de seguridad posible en el dispositivo móvil y de manera general, se recomienda disponer siempre de la última versión de todas las apps instaladas, independientemente del desarrollador. La última versión debería solucionar todas las vulnerabilidades de seguridad públicamente conocidas.

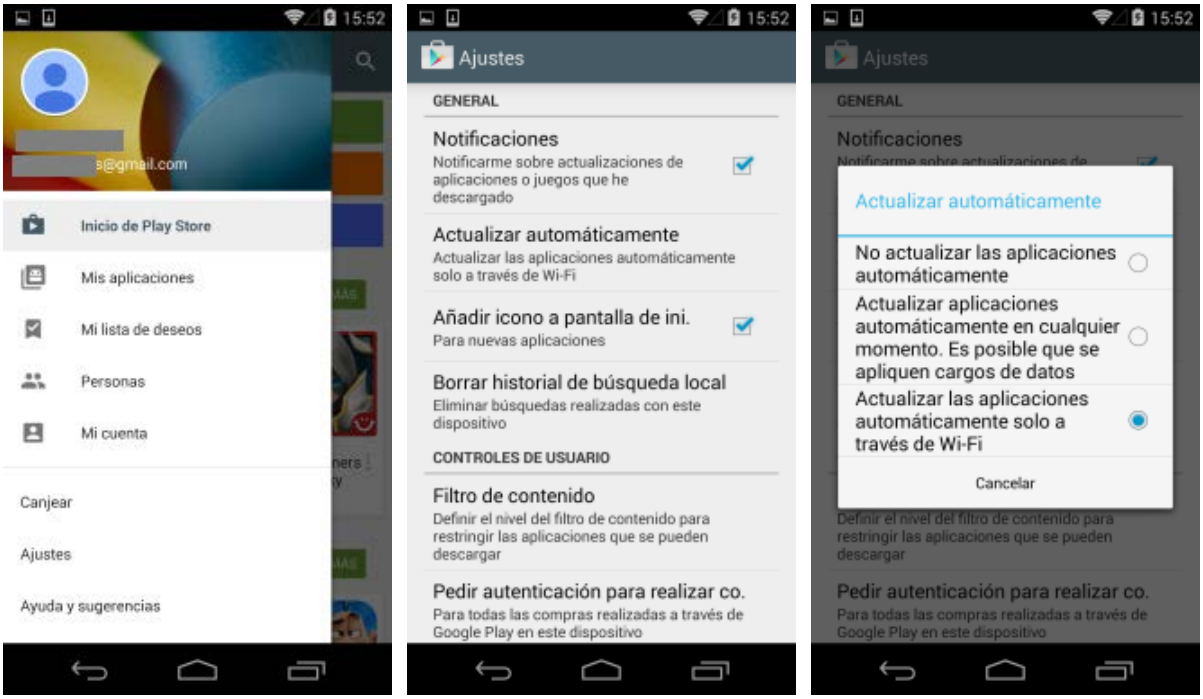
1281. La información respecto a las actualizaciones de software y descargas disponibles para las apps de Android está disponible en Google Play y/o en la página web de su desarrollador.

1282. La instalación de actualizaciones de software y apps en Android, si todas las apps se han obtenido a través de Google Play, tiene asociado un proceso homogéneo, facilitando el proceso de actualización para usuarios no experimentados y aumentando el nivel de seguridad de los dispositivos móviles al agilizar el proceso de sustitución de software vulnerable.

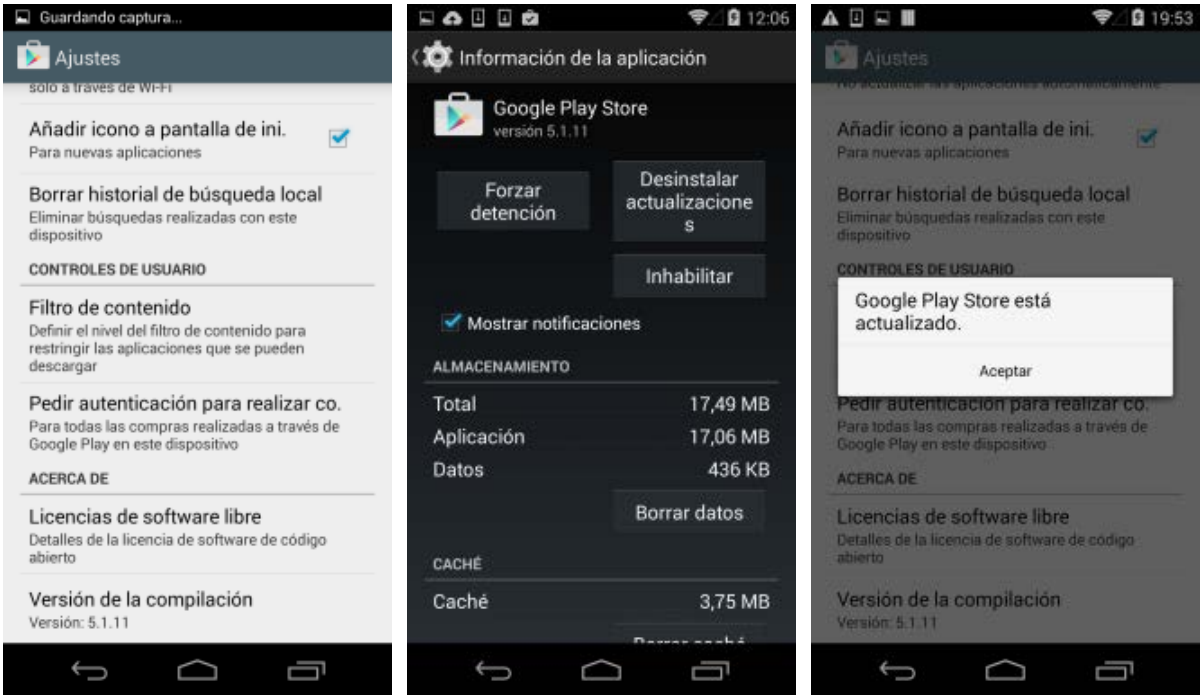
5.22.6 ACTUALIZACIONES AUTOMÁTICAS DE LAS APPS

1283. Android proporciona capacidades para actualizar automáticamente las apps instaladas en el dispositivo móvil tan pronto se detecte que hay disponible una nueva versión de las mismas en Google Play.

1284. Desde la app "Play Store", mediante el icono de menú es posible acceder a los "Ajustes" de Google Play. Desde la sección "General", es posible seleccionar la opción "Actualizar automáticamente":



1285. Como puede verse en el ejemplo, aunque la versión por defecto de la app "Play Store" en Android 4.4.4 es la versión 4.5.10, ésta ha sido actualizada automáticamente (y sin la intervención del usuario) a la versión 5.1.11:



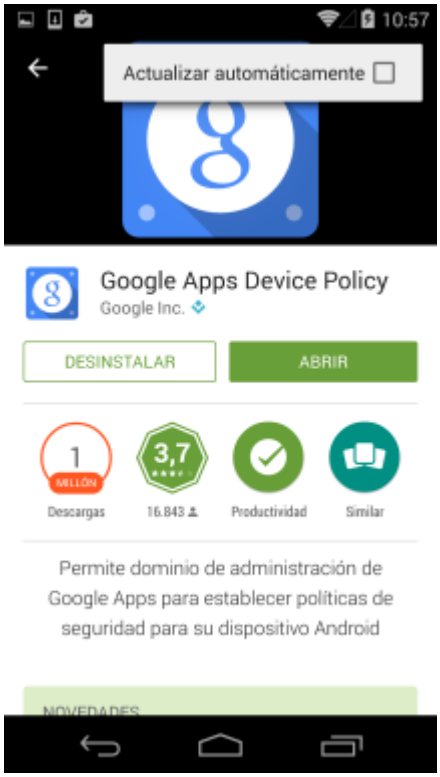
1286. Por defecto la funcionalidad de actualización automática de las apps en Google Play está habilitada sólo para llevarse a cabo mediante conexiones de datos a través de redes Wi-Fi. Adicionalmente, es posible definir si también es posible realizar las actualizaciones automáticas de las apps a través de la conexión de telefonía móvil (2/3/4G) del dispositivo móvil, ya que esta última puede tener costes asociados.

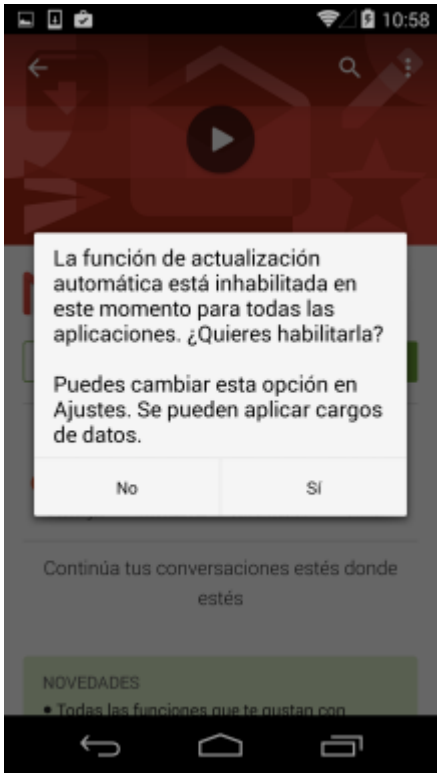
1287. Finalmente, también es posible deshabilitar las actualizaciones automáticas de las apps por completo, siendo necesaria la intervención manual del usuario para completar la

actualización de cualquier app. Se sugiere aplicar una configuración específica en base a las recomendaciones descritas posteriormente.

1288. Para ello debe modificarse la opción "Actualizar las aplicaciones automáticamente solo a través de Wi-Fi" (opción habilitada por defecto) disponible en la app "Play Store", desde el icono de menú, accediendo a los "Ajustes" de Google Play y, en concreto, a la sección "General" (mostrada en las imágenes previas).

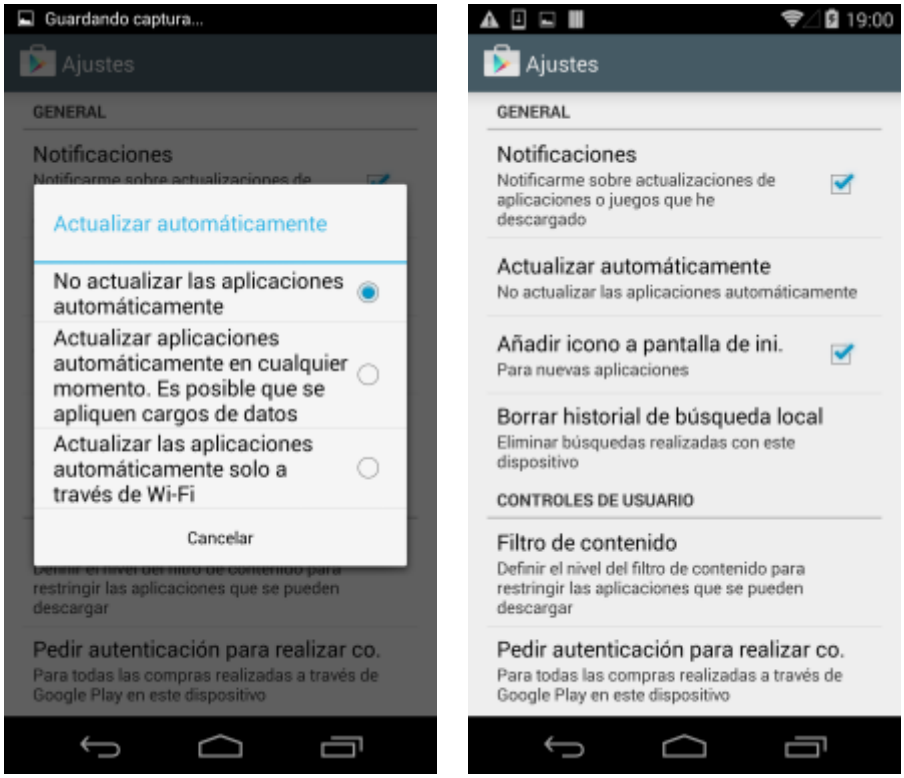
1289. Por otro lado, puede dar la impresión que pudiera existir la posibilidad de desactivar las actualizaciones automáticas para apps específicas, de manera individual [Ref.- 160]. Desde la app "Play Store", mediante el icono de menú es posible acceder a "Mis aplicaciones" y seleccionar las apps ya instaladas. Una vez se ha seleccionado una app concreta, a través del icono de menú, se puede habilitar o deshabilitar la opción "Actualizar automáticamente", sin embargo, esta opción es equivalente a la descrita previamente, y tiene carácter global, es decir, habilita la funcionalidad para todas las apps y no sólo para la app seleccionada:





1290. Si la funcionalidad de actualizaciones automáticas ha sido habilitada, las nuevas actualizaciones serán aplicadas sin la intervención del usuario si la actualización no modifica los permisos requeridos por la app o, más recientemente, incluso si la actualización requiere disponer de nuevos permisos pero estos están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app (ver apartado "5.2.2. Permisos simplificados y grupos de permisos de Google Play").

1291. Por tanto, pese a que para un usuario no avanzado sería recomendable dejar activadas las actualizaciones automáticas, con el objetivo de disponer siempre de la última versión de cada app, que supuestamente solucionará las vulnerabilidades conocidas públicamente, debido al nuevo modelo de permisos simplificados de Android (ver apartado "5.2.2. Permisos simplificados y grupos de permisos de Google Play"), es preferible llevar a cabo las actualizaciones de las apps manualmente:



1292. Se recomienda por tanto no dejar habilitada la opción de actualizaciones automáticas, e independientemente del perfil del usuario del dispositivo móvil, forzar al usuario a revisar manualmente los nuevos permisos solicitados por cada una de las actualizaciones recibidas para todas y cada una de las diferentes apps instaladas en el terminal.

1293. Especialmente, los usuarios avanzados deben estar interesados en no habilitar esta opción para poder revisar y analizar minuciosamente las actualizaciones disponibles, y sus "nuevos" permisos, antes de que éstas sean instaladas.

1294. En caso de que los permisos de la app hayan cambiado con la actualización, el proceso de actualización manual mostrará los nuevos permisos requeridos por la nueva versión de la app que deberán ser aprobados por el usuario durante la instalación de la actualización de la app. Sin embargo, recientemente, si los nuevos permisos requeridos por la app están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app, la actualización podrá ser instalada automáticamente sin la intervención del usuario.

5.22.7 ALMACENAMIENTO DE CREDENCIALES E INFORMACIÓN SENSIBLE EN APPS

1295. El almacenamiento de credenciales e información sensible en Android es uno de los elementos críticos qué debería ser tenido en cuenta por los desarrolladores de apps.

1296. Las apps pueden almacenar los datos en el almacenamiento interno (o *sandbox*) asociado a la app, dónde sólo ésta tiene acceso salvo que se haya realizado el proceso de *rooting* al dispositivo móvil (o se explote otra vulnerabilidad), en el almacenamiento compartido (o externo), dónde cualquiera puede acceder a ellos ya que pueden disponer de permisos globales de lectura y escritura, o empleando proveedores de contenidos, que pueden ser privados o exportados para permitir el acceso por parte de otras apps, estableciendo permisos de lectura y escritura [Ref.- 181].

1297. Adicionalmente, por defecto el almacenamiento de datos se lleva a cabo sin cifrar, es decir, las credenciales de acceso a diferentes servicios y otra información sensible será almacenadas en ficheros o bases de datos (SQLite) en claro [Ref.- 106], por ejemplo, dentro del *sandbox* de la app bajo el directorio "/data/data".

1298. Si un atacante obtiene acceso físico al dispositivo móvil, podría seguir el proceso de *rooting* (o explotar otra vulnerabilidad) y disponer potencialmente de acceso a las credenciales lamacenadas sin cifrar.

1299. Se recomienda por tanto que los desarrolladores de apps almacenen los datos cifrados empleando una clave que no es accesible directamente por la app, por ejemplo, almacenándola en un KeyStore (ver apartado "5.7.1. Almacenamiento de credenciales") protegido por una contraseña que debe ser proporcionada por el usuario y que nunca es almacenada en el dispositivo móvil [Ref.- 181].

1300. Adicionalmente, se recomienda hacer uso de los mecanismos de cifrado del dispositivo móvil disponibles por defecto en Android 3.0+ (ver apartado "5.6.1. Cifrado del dispositivo móvil").`

5.23 INSTALACIÓN Y ELIMINACIÓN DE APPS EN ANDROID

1301. Las apps para Android están desarrolladas en el lenguaje de programación Java y ejecutan sobre una máquina virtual Java ligera denominada Dalvik [Ref.- 16].

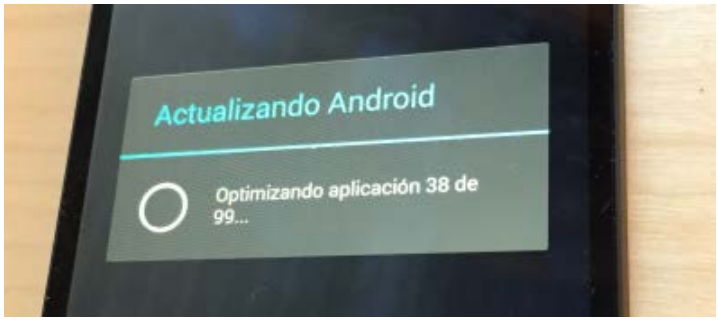
1302. La máquina virtual Dalvik ha sido optimizada para su utilización en dispositivos móviles, con un consumo eficiente de memoria y de recursos. Dalvik ejecuta ficheros en formato Dalvik Executable (.dex), o DEX, por lo que en el proceso de desarrollo el código fuente Java (ficheros ".java", asociado posteriormente a ficheros ".class", Java *bytecode*) de las apps de Android es convertido al formato DEX, Dalvik bytecode (mediante la herramienta "dx").

1303. Android 4.4 (KitKat) introdujo el nuevo entorno de ejecución ART (Android RunTime) como sustituto de Dalvik VM, pero todavía de manera experimental y no habilitado por defecto.

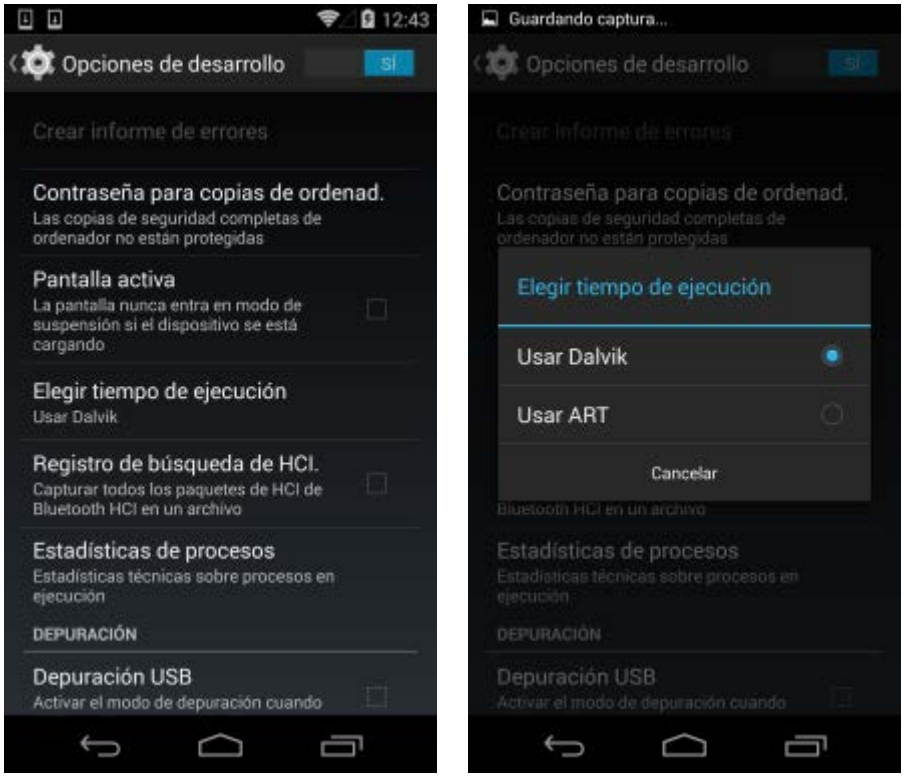
1304. ART es un entorno de ejecución (utilizado tanto por las apps como por algunos servicios de sistema de Android) compatible con Dalvik, que ejecuta binarios en el formato DEX.

1305. Una de sus principales ventajas es que hace uso de una técnica conocida como compilación AOT (Ahead-of-Time), que mejora el rendimiento de la ejecución de las apps. Cuando se instala una nueva app en Android, ART, a través de la herramienta "dex2oat", compila el código DEX de la app en código ejecutable nativo (por ejemplo, ARM) para la plataforma específica del dispositivo móvil (en concreto, en ficheros ".oat" [Ref.- 193]).

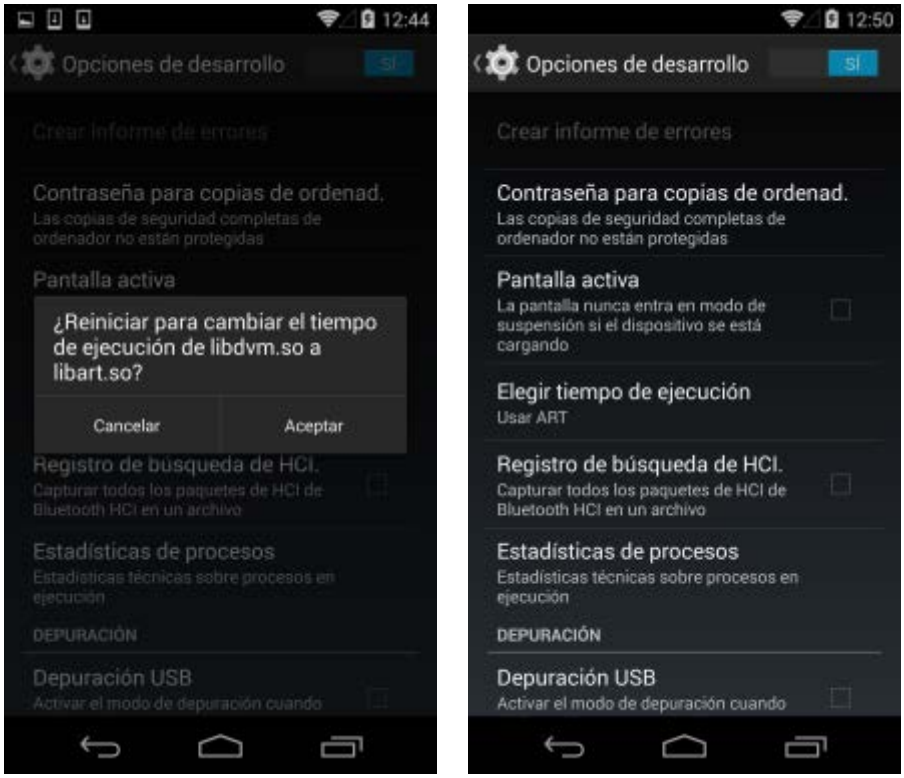
1306. Como resultado, la primera vez que arranca el dispositivo móvil tras habilitar ART, llevará a cabo el proceso de conversión de las diferentes apps disponibles. Por este motivo el proceso de arranque puede llevar unos minutos, en función del número de apps instaladas, mostrándose el mensaje, por ejemplo, "Optimizando aplicación 33 de 99...":



1307. En Android 4.4 es posible hacer uso de ART modificando la configuración por defecto del dispositivo móvil, desde el menú "Ajustes [Sistema] - Opciones de desarrollo", y en concreto mediante la opción "Elegir tiempo de ejecución" (ver apartado "5.11.3. Opciones de desarrollo y depuración USB"):



1308. Al cambiar el entorno de ejecución de Dalvik a ART, Android solicita reiniciar el dispositivo móvil para empezar a hacer uso de la librería "libart.so" en lugar de "libdvm.so":



1309. Las herramientas de desarrollo de software de Android (Android SDK, *Software Development Kit*, o Android SDK Tools, y Android Studio[114] [Ref.- 22]) generan las apps para Android, o paquetes Android, en un único archivo o contenedor con extensión ".apk" (Android PacKage).

1310. Adicionalmente al código Java, Android permite el desarrollo de aplicaciones nativas (ARM) usando C/C++, mediante el Android NDK (*Native Development Kit*), o híbridas, es decir, aquellas que contienen tanto código Java como código nativo (y hacen uso del Java Native Interface, JNI).

1311. Todas las apps para Android deben ser firmadas digitalmente por su desarrollador mediante certificados digitales, siendo por tanto posible identificar (teóricamente) al desarrollador de cualquier app oficial (ver apartado "5.2.4. Firma digital de apps en Android").

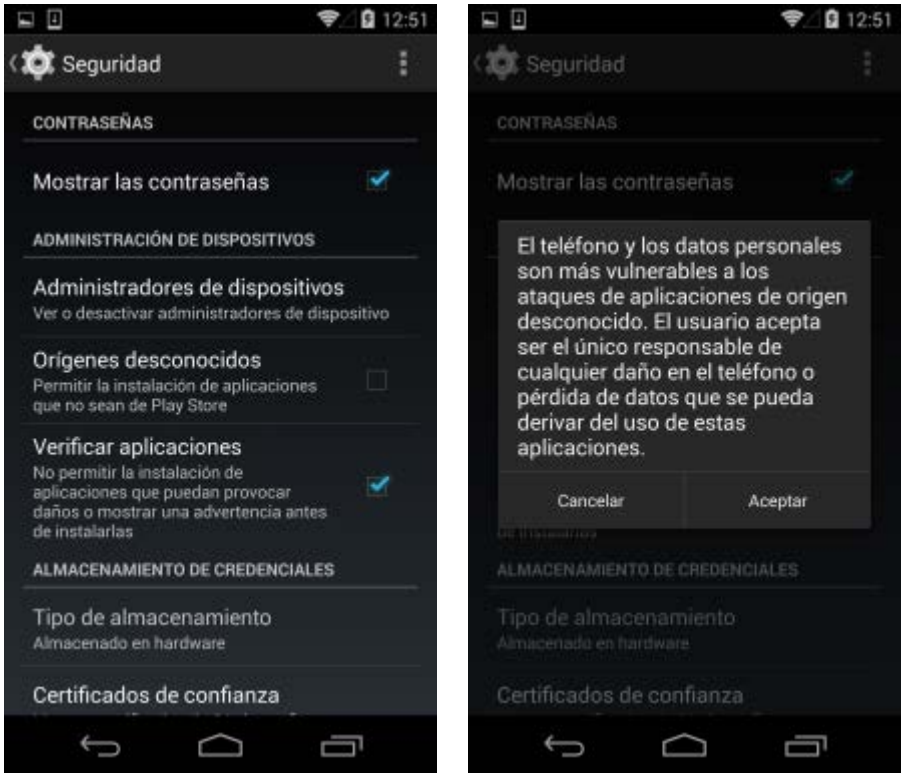
1312. La firma de las apps es empleada adicionalmente por Android para establecer permisos de operaciones entre apps y distintos niveles de protección [Ref.- 102] (según el fichero *manifest*), y para permitir a las apps compartir su ID (si han sido programadas y firmadas por el mismo desarrollador).

1313. El módulo estándar de instalación de apps de Android verifica mediante certificados digitales que las apps oficiales, es decir, que provienen de Google Play, han sido firmadas convenientemente por su desarrollador.

1314. Adicionalmente, es posible configurar el dispositivo móvil para permitir la instalación de apps no oficiales (no provenientes de Google Play) sin para ello ser necesario realizar el proceso de *rooting* sobre el terminal.

[114] http://developer.android.com/sdk/index.html

1315. Para permitir la instalación de cualquier app, incluso proveniente de fuentes que no son de confianza, simplemente es necesario eliminar las comprobaciones de seguridad asociadas en Android mediante la opción "Orígenes desconocidos" del menú "Ajustes [Personal] - Seguridad [Administración de dispositivos]":



1316. Desde el punto de vista de seguridad y con el objetivo de evitar la instalación de apps de fuentes desconocidas, o que no son de confianza, se recomienda no habilitar esta opción, tal como advierte el mensaje mostrado por Android (ver imagen superior derecha).

5.23.1 INSTALACIÓN REMOTA DE APPS

1317. En mayo de 2010 Google presentó la versión web de Google Play [Ref.- 4], que permite la consulta e instalación de apps en los dispositivos móviles Android desde otros ordenadores mediante un navegador web, en lugar de emplear la app de acceso al mercado oficial ("Play Store") desde los propios dispositivos móviles.

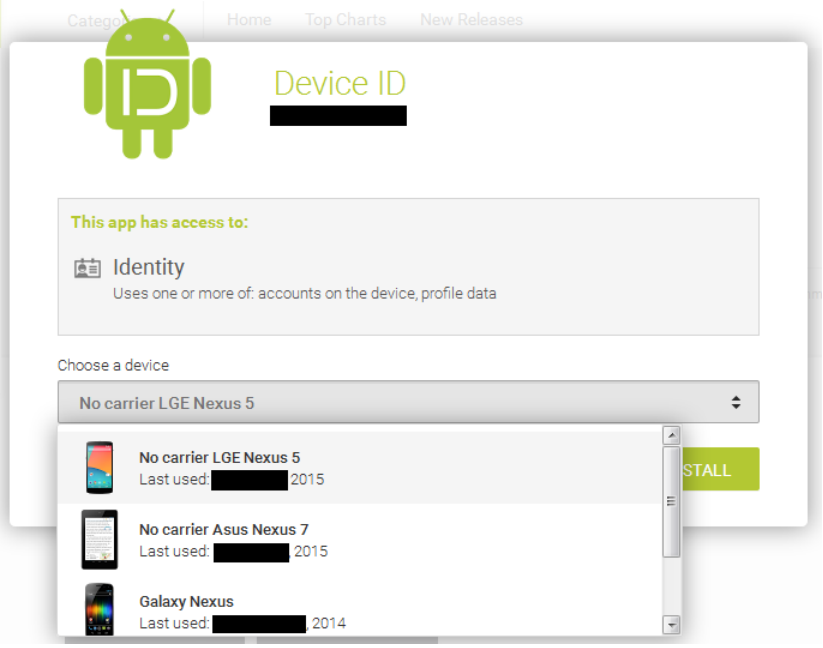
1318. Una vez se adquiere una app a través de la versión web de Google Play desde el mercado oficial de apps, Google se encarga de instalarla en el dispositivo móvil a través de una conexión persistente disponible en los dispositivos móviles basados en Android a través de Internet (ver apartado “5.23.3. Conexión GTalkService”).

1319. La conexión permanente a través de Internet disponible entre los dispositivos móviles Android y Google se basa en el GTalkService [Ref.- 77]. Para la instalación remota de apps se emplea un mecanismo de envío de mensajes propio de Google y Android, y en concreto en este caso, el mensaje denominado INSTALL_ASSET [Ref.- 78].

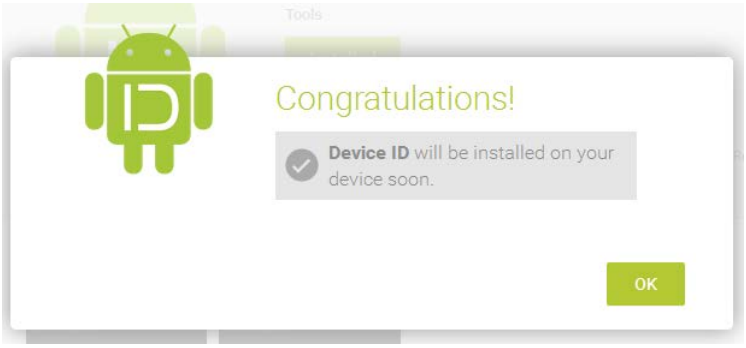
1320. Antes de llevar a cabo la instalación de cualquier nueva app, se recomienda revisar y analizar exhaustivamente los permisos solicitados por la misma sobre el dispositivo móvil.

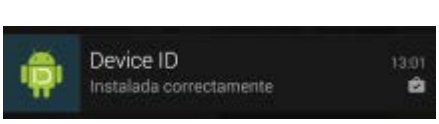
1321. El acceso a Google Play se realiza mediante la cuenta de usuario de Google, por lo que el acceso no autorizado por parte de un atacante a dicha cuenta permitiría la instalación de apps en el dispositivo móvil asociado del usuario [Ref.- 8].

1322. Tras seleccionar la app en la web de Google Play, el usuario puede seleccionar en cuál de los diferentes dispositivos móviles vinculados a la cuenta de usuario de Google se desea realizar su instalación:



1323. Tras confirmar su instalación en el dispositivo móvil seleccionado, se obtiene la confirmación a través de la página web de Google Play, y en el dispositivo móvil el proceso de instalación se lleva a cabo automáticamente, y conlleva únicamente un aviso en la barra de notificaciones del dispositivo (y la aparición del icono de la app en algunas de las pantallas de inicio):





1324. Alternativamente, podría ser posible la instalación remota de apps desde la web de Google Play de forma no autorizada si un potencial atacante obtiene los identificadores de sesión empleados en el acceso web a Google Play del usuario [Ref.- 75].

5.23.2 ELIMINACIÓN REMOTA DE APPS

1325. Los dispositivos móviles basados en Android disponen también de capacidades por parte del vendedor, Google/Android, para eliminar apps de los mismos de forma remota.

1326. Este mecanismo fue diseñado como medida de seguridad en situaciones de emergencia para poder proteger a los usuarios en caso de que se produzca una distribución masiva de apps dañinas o maliciosas concretas.

1327. En junio de 2010 Google empleó estas capacidades por primera vez [Ref.- 5] [Ref.- 78] para eliminar una app creada como prueba de concepto que pretendía demostrar la facilidad para introducir apps maliciosas en los mercados de aplicaciones de varios fabricantes de dispositivos móviles, incluyendo Android Market (nombre empleado para Google Play en aquél momento).

1328. Posteriormente, Google ha hecho uso de esta funcionalidad en (al menos) otra ocasión para eliminar otras apps maliciosas introducidas en Android Market. Por ejemplo, en marzo de 2011, se vieron afectadas unas 50 aplicaciones infectadas con malware bajo el nombre de DroidDream que fueron instaladas en más de 200.000 dispositivos móviles (cifras no oficiales) [Ref.- 6]. Estas apps hacían uso de vulnerabilidades conocidas en versiones de Android previas a la versión 2.2.2, y específicamente, técnicas empleadas habitualmente para conseguir acceso como root a dispositivos móviles Android (proceso conocido como *root*, *rooted* o *rooting* del dispositivo Android).

1329. Esas capacidades permiten a Google no sólo eliminar las apps maliciosas de Google Play y suspender las cuentas de los desarrolladores sospechosos, sino también eliminar las apps de los dispositivos móviles de los usuarios donde han sido instaladas, notificando al usuario sobre las acciones realizadas.

1330. La conexión persistente entre Google y los dispositivos móviles basados en Android también podría permitir la instalación remota de apps, y se emplea en la instalación de apps adquiridas desde el interfaz web de Google Play (detallada en el apartado previo).

5.23.3 CONEXIÓN GTALKSERVICE

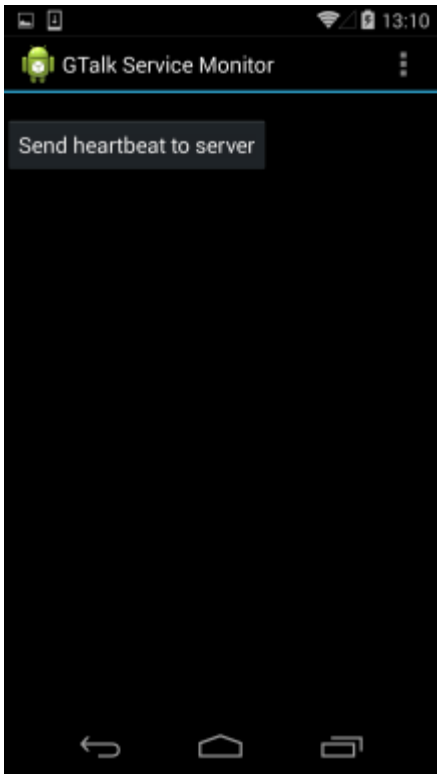
1331. La conexión GTalkService [Ref.- 77] [Ref.- 78], comunicación permanente a través de Internet disponible entre los dispositivos móviles Android y Google, emplea los protocolos TCP/SSL/XMPP para comunicarse periódicamente con los servidores de Google (mtalk.google.com) en el puerto TCP/5228 haciendo uso de las conexiones de datos del terminal, telefonía móvil (2/3/4G) o Wi-Fi.

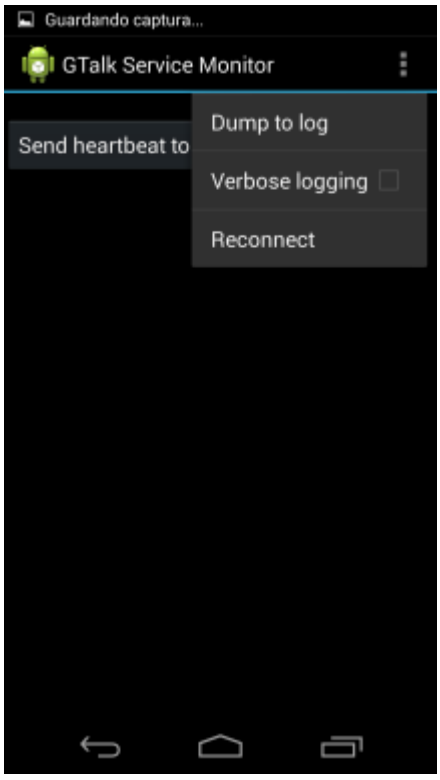
1332. El servicio GTalkService es empleado para el envío de mensajes desde Google a los dispositivos móviles Android, o para la instalación o eliminación remota de apps.

1333. El protocolo empleado por GTalkService no hace uso de mecanismos adicionales de seguridad (por ejemplo, firmas criptográficas de los mensajes intercambiados) aparte del uso de HTTPS (SSL/TLS), por lo que un ataque sobre este protocolo permitiría potencialmente modificar el trafico intercambiado y, por ejemplo, eliminar o instalar nuevas apps en el dispositivo móvil.

1334. Mediante el código *#*#8255#*#* (o *#*#talk#*#*) del teclado del teléfono en Android es posible ejecutar el GTalk Service Monitor, una aplicación de depuración que permite obtener todos los detalles de ejecución de GTalkService.

1335. Por defecto, en Android 4.4.4, los detalles de este servicio están ocultos[115], y ni siquiera se pueden obtener los detalles de este servicio a través del botón de menú, y de la opción "Verbose logging":





1336. En versiones previas de Android, como 2.x, el *Gtalk Service Monitor* disponía de múltiples pantallas con información del servidor y puerto al que se encuentra conectado el dispositivo móvil, el identificador de usuario (Google JID) y de dispositivo móvil (Device ID), el intervalo de comprobación de la conexión (15 minutos), el estado de la conexión, un histórico de conexiones, o estadísticas de la transmisión de datos y las comunicaciones.

Nota: los valores del "JID" (ejemplo, "usuario@gmail.com/android<CODIGO>", dónde <CODIGO> es un string de 12 valores hexadecimales) y del "Device ID" (ejemplo, "android-<CODIGO>", dónde <CODIGO> es un string de 16 valores hexadecimales) no están relacionados con el valor del "ANDROID_ID" (ver apartado "5.9. Configuración por defecto del dispositivo móvil").

1337. Periódicamente, el dispositivo móvil comprueba que la conexión GTalkService continúa activa (*heartbeat*). Mediante el Gtalk Service Monitor es posible forzar una comprobación o *heartbeat* (botón "Send heartbeat to server").

1338. El *heartbeat* requiere de tres o cuatro paquetes TCP (correspondientes a un intercambio de datos por cada extremo más las correspondientes confirmaciones) asociados a la sesión existente de GTalkService para realizar la comprobación del estado de la conexión:

```
182 942.984695 192.168.1.170  209.85.227.188  TCP  49831 > hpvroom [PSH, ACK] Seq=659 Ack=261 Win=6912 Len=37 TSV=1485357 TSER=328908344
183 943.056020 209.85.227.188 192.168.1.170   TCP  hpvroom > 49831 [ACK] Seq=261 Ack=696 Win=6784 Len=0 TSV=329808362 TSER=1485357
184 943.056857 209.85.227.188 192.168.1.170   TCP  hpvroom > 49831 [PSH, ACK] Seq=261 Ack=696 Win=6784 Len=37 TSV=329808362 TSER=1485357
185 943.060447 192.168.1.170  209.85.227.188  TCP  49831 > hpvroom [ACK] Seq=696 Ack=298 Win=6912 Len=0 TSV=1485366 TSER=329808362
```

[115] A diferencia de como ocurría en versiones previas de Android, 2.x (ver la versión previa de la presente guía).

5.23.4 VERIFICACIÓN DE SEGURIDAD DE LAS APPS

1339. Por un lado, Google lleva a cabo un proceso de escaneo o verificación de seguridad automático sobre las apps que son publicadas por los desarrolladores a través de Google Play. Para ello hace uso de un sistema de análisis denominado Google Bouncer, y cuyo principal propósito es identificar apps que contienen software malicioso (*malware*).

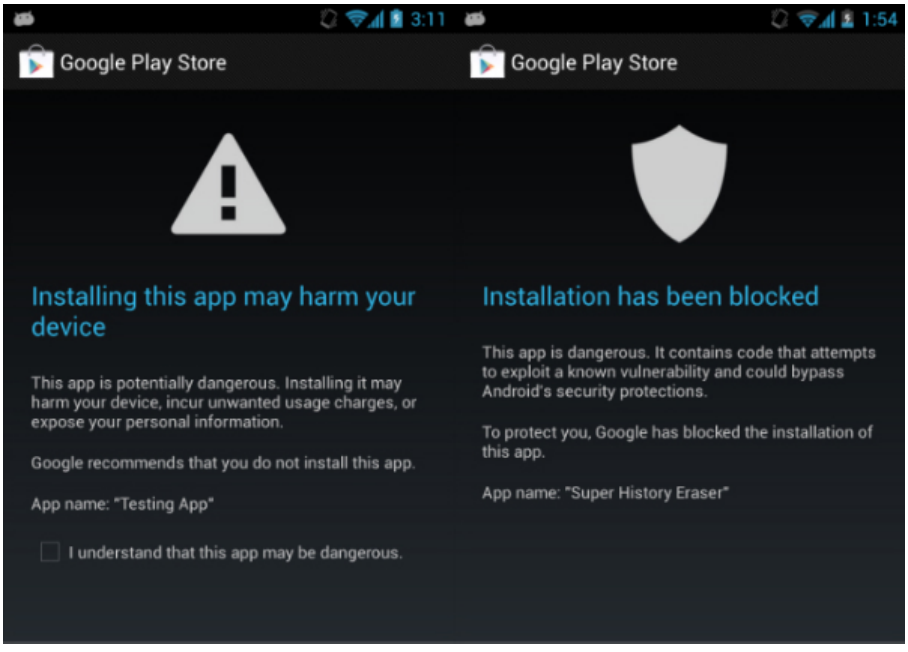
1340. Google Bouncer [Ref.- 166] compara cada app con otras muestras de software malicioso conocidas, y también ejecuta las apps en un entorno virtual, simulando su ejecución en un dispositivo móvil Android, para analizar su comportamiento antes de proceder a su publicación oficial, e intentando identificar comportamientos maliciosos o anómalos normalmente asociados al *malware*.

1341. El sistema Google Bouncer analiza nuevas apps, apps existentes previamente en Google Play, reanaliza apps ya analizadas previamente una vez se incorporan nuevas capacidades al sistema, y también analiza cuentas de desarrolladores de Android (especialmente las de los nuevos desarrolladores, para evitar que agentes que distribuyen *malware* para Android lo hagan empleando la identidad de otros supuestos nuevos desarrolladores).

1342. Por otro lado, Android 4.4 (desde la versión 4.2 de Android) dispone de capacidades para el escaneo o verificación de seguridad de las apps durante el proceso de instalación, con el objetivo de identificar y detectar la existencia de software malicioso (*malware*) en las mismas, característica conocida (en inglés) como "Verify Apps" [Ref.- 169].

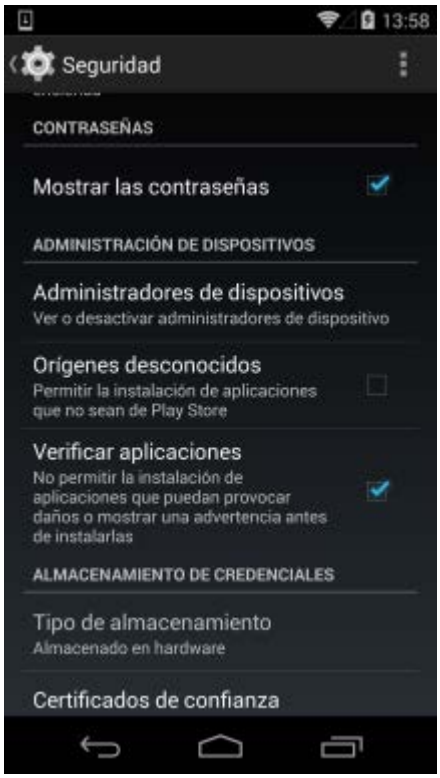
1343. Las capacidades de verificación de apps comparan la app a instalar con una base de datos de apps existente en Google, con el objetivo de identificar si corresponde a un app conocida con comportamiento malicioso o dañino. El proceso de verificación envía a Google información sobre el nombre de la app, su tamaño, su *hash* SHA1, la versión y la URL asociada [Ref.- 170].

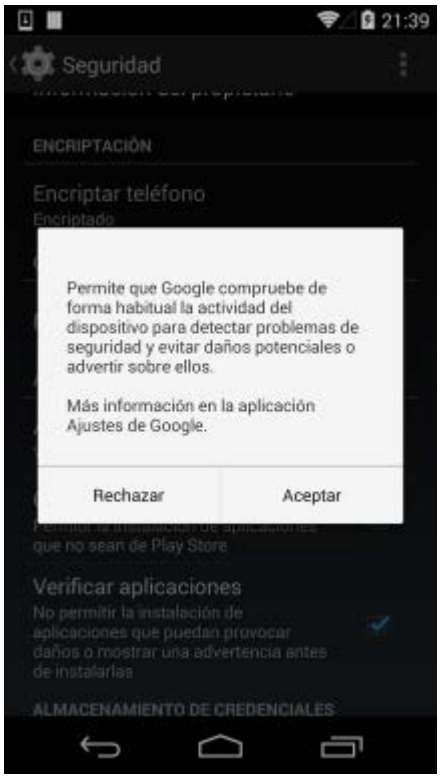
1344. En caso de identificarse la app como dañina, en función del nivel de peligrosidad asociado a la app, Android puede recomendar al usuario que no instale la app (en el caso de apps potencialmente dañinas), o incluso llegar a bloquear la app (en el caso de apps dañinas), no siendo posible proceder con su instalación [Ref.- 167] (ejemplos en inglés):



1345. Esta verificación se lleva a cabo para las apps que son instaladas manualmente por el usuario, por ejemplo desde una página web, un mercado de apps de Android no oficial, o a través de ADB (proceso conocido como *sideload*). Para las apps instaladas desde Google Play se confía en la verificación realizada por Google Bouncer (descrito previamente).

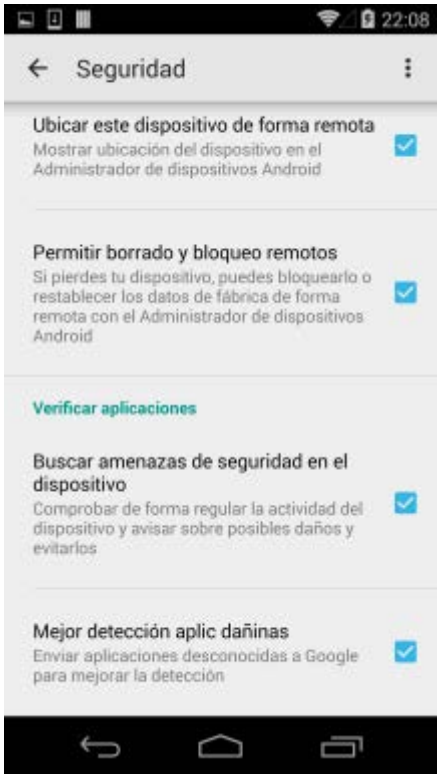
1346. Para que las capacidades de verificación de apps entren en funcionamiento (además de permanecer habilitadas) es necesario haber habilitado también previamente la posibilidad de instalar apps de fuentes que no son de confianza, mediante la opción "Orígenes desconocidos" (ver apartado "5.23. Instalación y eliminación de apps en Android"):





1347. Este matiz es fundamental, ya que si la opción de "Orígenes desconocidos" no está activada, es aún posible instalar apps vía ADB (si se han permitido las opciones de desarrollo y la depuración vía USB) sin que se active la funcionalidad de verificación de apps.

1348. La primera vez que se instala una app desde una fuente que no es de confianza, Android mostrará una pantalla solicitando al usuario la capacidad para enviar a Google, como parte de la funcionalidad "Verify Apps", información sobre el dispositivo móvil (como por ejemplo URLs asociadas a la app, el identificador del dispositivo móvil, la versión de Android, la dirección IP, cookies, etc):

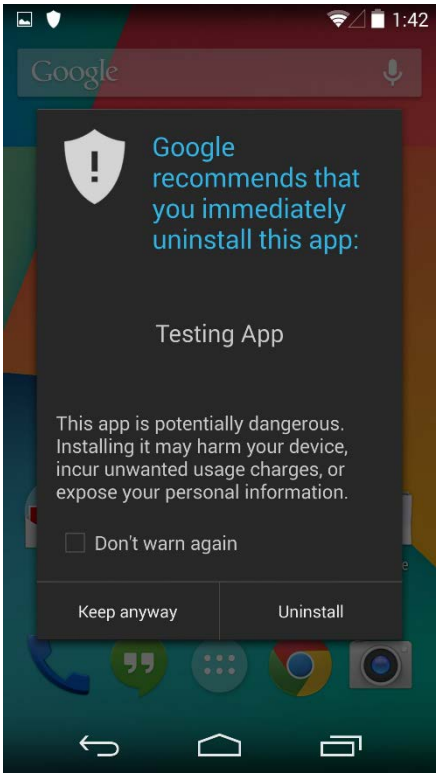


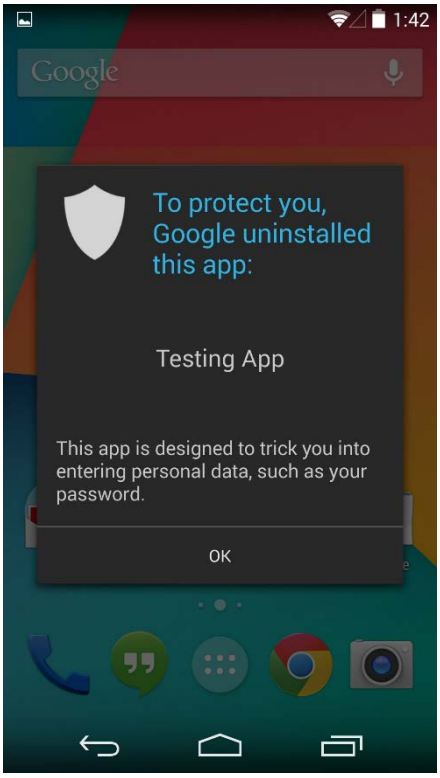
Nota: la apariencia gráfica de la pantalla previa, más en la línea del diseño *Material* asociado a Android 5.x (Lollipop), pese a estar haciendo uso de Android 4.4.4 (KitKat), se debe a la utilización de una versión de los servicios de Google Play (y de la app "Play Store") actualizada, en concreto la versión 5.1.11.

1349. Adicionalmente, al activar la verificación de apps, Google recopilará información (supuestamente) anónima sobre las apps que son instaladas desde fuera de Google Play, con el objetivo de mejorar la detección de apps dañinas [Ref.- 169].

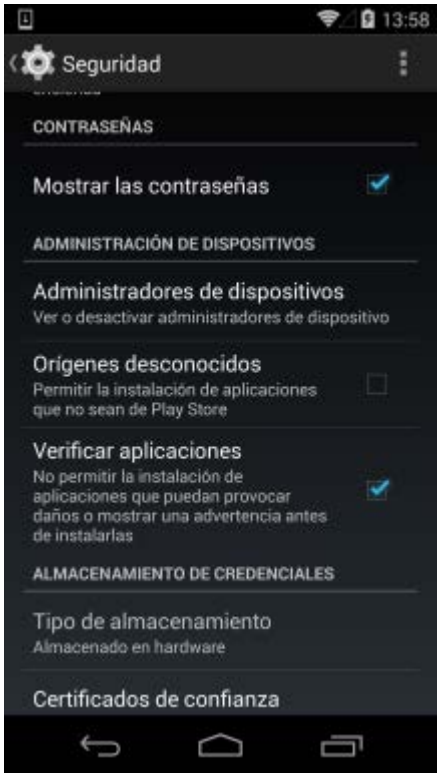
1350. Las últimas versiones de la funcionalidad "Verify Apps" no sólo analizan las apps en el momento de su instalación, sino que también las comprueban y monitorizan periódicamente durante su ejecución, por si presentan algún comportamiento inesperado que no fue detectado durante la instalación [Ref.- 168]. En caso de identificarse la app como dañina, Android puede recomendar al usuario que desinstale la app o incluso llegar a eliminar la app del dispositivo móvil[116]:

[116] Imágenes: http://www.businessinsider.com/google-verify-apps-for-android-phones-2014-4



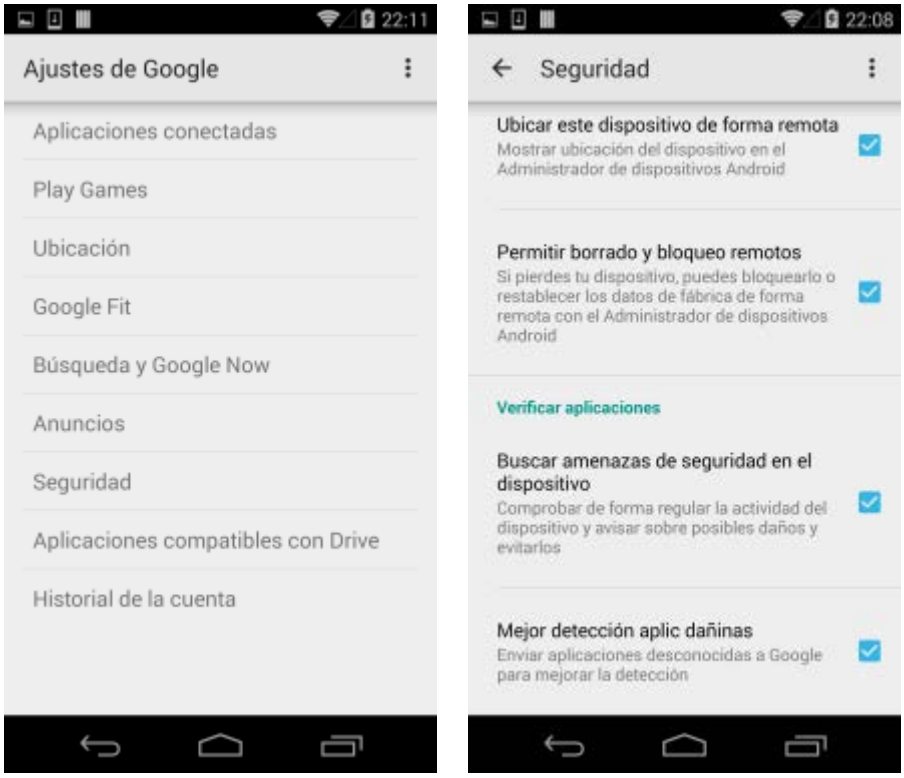


1351. Las capacidades de verificación de apps se encuentran habilitadas por defecto en Android 4.4.4 (no necesariamente en versiones previas de Android 4.2.x o superior), y pueden ser deshabilitadas (opción no recomendada desde el punto de vista de seguridad) a través de la opción "Verificar aplicaciones" del menú "Ajustes [Personal] - Seguridad [Administración de dispositivos]":



1352. En el caso de dispositivos móviles Android multiusuario, únicamente el usuario propietario podrá activar o desactivar la verificación de apps.

1353. Las opciones adicionales de configuración de la funcionalidad de verificación de apps (mencionados previamente) están disponibles a través de la app de "Ajustes de Google", dentro de la sección "Seguridad" y bajo la sección "Verificar aplicaciones". La opción "Buscar amenazas de seguridad en el dispositivo" permite habilitar o deshabilitar las capacidades de verificar periódicamente las apps (y no sólo en el momento de su instalación), mientras que la opción "Mejor detección aplicaciones dañinas" permite habilitar o deshabilitar el envío de información de las apps desconocidas a Google para mejorar las capacidades de detección. Ambos ajustes de configuración están activos por defecto:



Nota: la apariencia gráfica de las pantallas previas, más en la línea del diseño *Material* asociado a Android 5.x (Lollipop), pese a estar haciendo uso de Android 4.4.4 (KitKat), se debe a la utilización de una versión de los servicios de Google Play (y de la app "Play Store") actualizada, en concreto la versión 5.1.11 (que también modifica la app de "Ajustes de Google"), tal como ya ha sido mencionado previamente.

1354. Desde el punto de vista de seguridad se recomienda dejar habilitada la primera de las opciones, para disponer de una verificación más regular y continua, y activar únicamente la segunda opción si se desea colaborar con Google en el proceso de detección de *malware*.

1355. Pese a que estas capacidades fueron introducidas en Android 4.2, actualmente están también disponibles para dispositivos móviles incluso basados en Android 2.3 (o superior) a través de la actualización de los servicios de Google Play. Por tanto, otros dispositivos móviles Android más antiguos, incluso aunque no dispongan de la versión Android 4.4 (KitKat), pueden disponer de estas capacidades de escaneo o verificación de apps (ver apartado "5.23.4. Verificación de seguridad de las apps"), ya que las mismas fueron introducidas por Google en una de las actualizaciones del componente (y app) asociado a

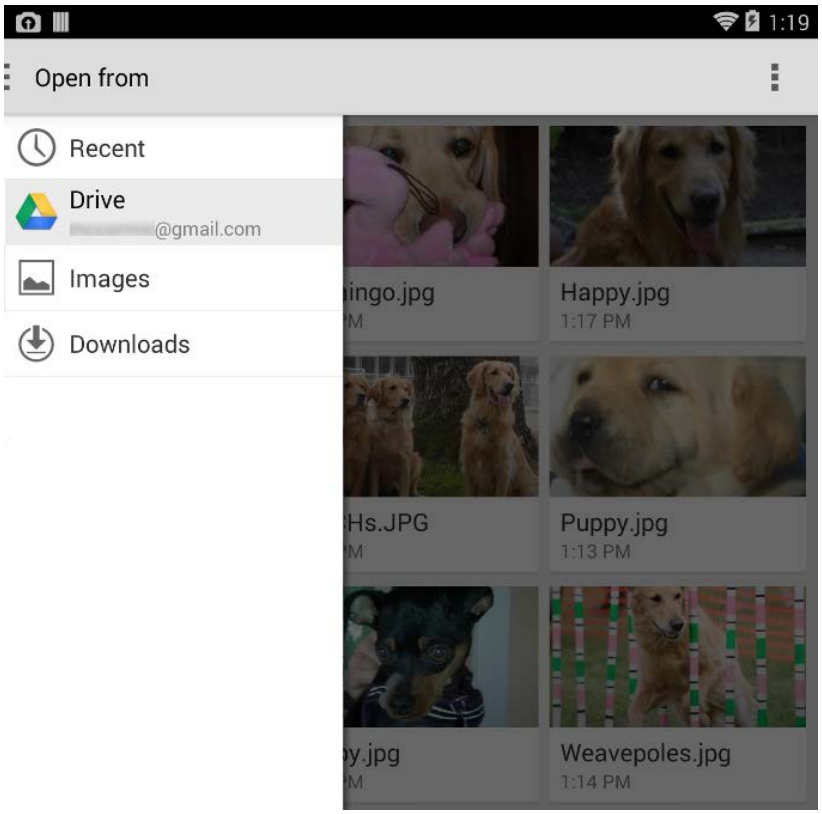
los servicios de Google Play[117] (sin ser necesario realizar una actualización de la versión del sistema operativo).

1356. Debe tenerse en cuenta que tanto las capacidades introducidas por Google Bouncer [Ref.- 171], como las asociadas a "Verify Apps" [Ref.- 170], añaden niveles de seguridad adicionales, bajo el paradigma de seguridad en profundidad (es decir, añadir varios niveles o capas de protección), pero no proporcionan una protección completa (no son efectivas al 100%), pudiendo existir técnicas para evadir estos mecanismos de verificación de seguridad (tal como ya han demostrado en el pasado los estudios referenciados).

5.23.5 ACCESO Y ALMACENAMIENTO DE DATOS DESDE APPS

1357. Android 4.4 introdujo el *Storage Access Framework* (SAF), un entorno que simplifica el acceso, edición y almacenamiento de documentos, imágenes, vídeos y otros ficheros por parte de las apps de Android, con la capacidad de emplear múltiples proveedores de almacenamiento o proveedores de documentos (*Document Providers*).

1358. Los servicios o proveedores de almacenamiento pueden ser tanto locales (memoria interna del dispositivo) como pertenecer a servicios de almacenamiento en la nube (como por ejemplo Google Drive, One Drive, Dropbox, Box, etc), y las apps pueden obtener, modificar, borrar, crear y guardar ficheros o documentos en ellos de manera homogénea a través de un interfaz estándar y unificado, así como acceder y compartir documentos proporcionados por otras apps existentes en el dispositivo móvil a través de SAF [Ref.- 162]:



[117] http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/

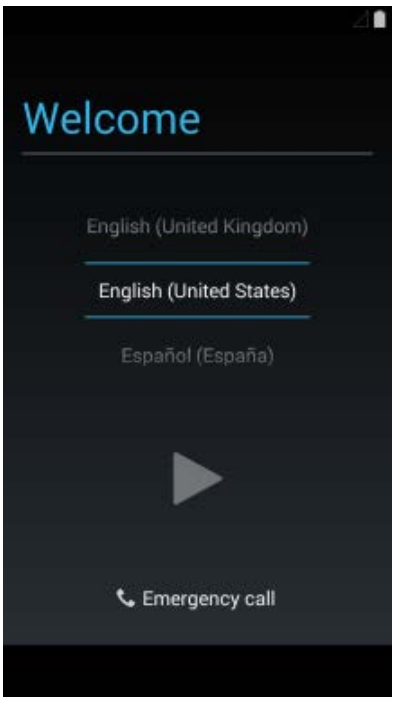
1359. Estas nuevas capacidades influyen principalmente en las capacidades disponibles para los desarrolladores de apps para Android, permitiéndoles gestionar múltiples documentos o hacerlo individualmente, establecer permisos sobre estos, y gestionar la autentificación del usuario en los servicios de almacenamiento en la nube antes de realizar operaciones con los datos a guardar o gestionar.

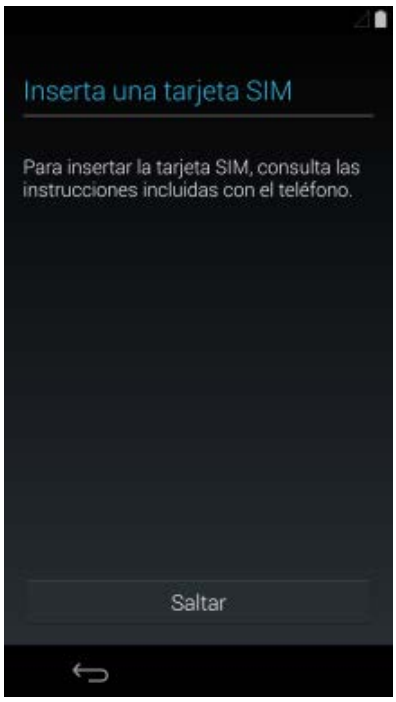
1360. Para el usuario del dispositivo móvil, los detalles de dónde y cómo se almacenan los documentos por parte de las apps son prácticamente transparentes, por lo que únicamente debe prestar especial atención desde el punto de vista de seguridad a si desea almacenar los documentos sólo localmente, o en algún servicio en la nube.

6. APÉNDICE A: PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL

1361. El presente apartado detalla el proceso de instalación y configuración inicial de Android 4.x al encender por primera vez el dispositivo móvil tras su adquisición (o tras restablecer los ajustes de fábrica).

1362. Al arrancar el dispositivo móvil, se muestra una pantalla de bienvenida, "Welcome" ("Te damos la bienvenida"), donde se debe seleccionar el idioma con el que se desea configurar el dispositivo y que también se empleará durante el proceso de instalación (por ejemplo, "Español (España)":





1363. A continuación se muestra la pantalla que insta al usuario a insertar una tarjeta SIM, "Inserta una tarjeta SIM", proceso opcional que puede ser evitado mediante el botón "Saltar" (ver imagen superior derecha) si no se desea hacer uso de las redes de telefonía móvil en este momento.

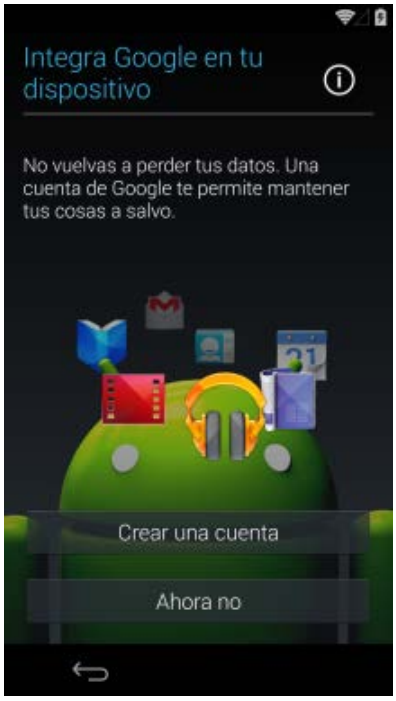
1364. Para configurar las diferentes opciones y ajustes de configuración del dispositivo móvil, es necesario disponer de conectividad a Internet mediante la selección de una red Wi-Fi, "Selecciona una red Wi-Fi", aunque este paso también es opcional (mostrándose de nuevo el botón "Saltar"):

1365. Las opciones de configuración avanzada, disponibles a través del botón superior derecho con tres puntos ("..."), botón de menú, permiten configurar una red Wi-Fi que haga uso de WPS, mientras que la opción inferior "+ Otra red..." permite conectarse a redes Wi-Fi ocultas que no aparecen en la lista actual de redes visibles bajo el alcance del dispositivo móvil. Se desaconseja el uso de redes Wi-Fi ocultas desde el punto de vista de seguridad.

1366. En el caso de no seleccionar una red Wi-Fi, botón "Saltar", se muestra un mensaje de aviso que indica que hasta que no se disponga de conexión a Internet el dispositivo móvil no podrá verificar actualizaciones de software. Si pese a ello se omite este paso ("Omitir de todas formas"), se continúa con el proceso de instalación:

1367. Debe tenerse en cuenta que tanto si se omite el proceso de conexión a una red Wi-Fi, como si se establece una conexión con una red Wi-Fi (incluso aunque posteriormente se interrumpa el proceso de configuración inicial), el interfaz Wi-Fi será habilitado y permanecerá en ese estado tras el proceso de instalación y configuración inicial de Android 4.x. Se recomienda por tanto deshabilitar el interfaz Wi-Fi lo antes posible y proceder a su configuración siguiendo las recomendaciones del apartado "5.14. Comunicaciones Wi-Fi".

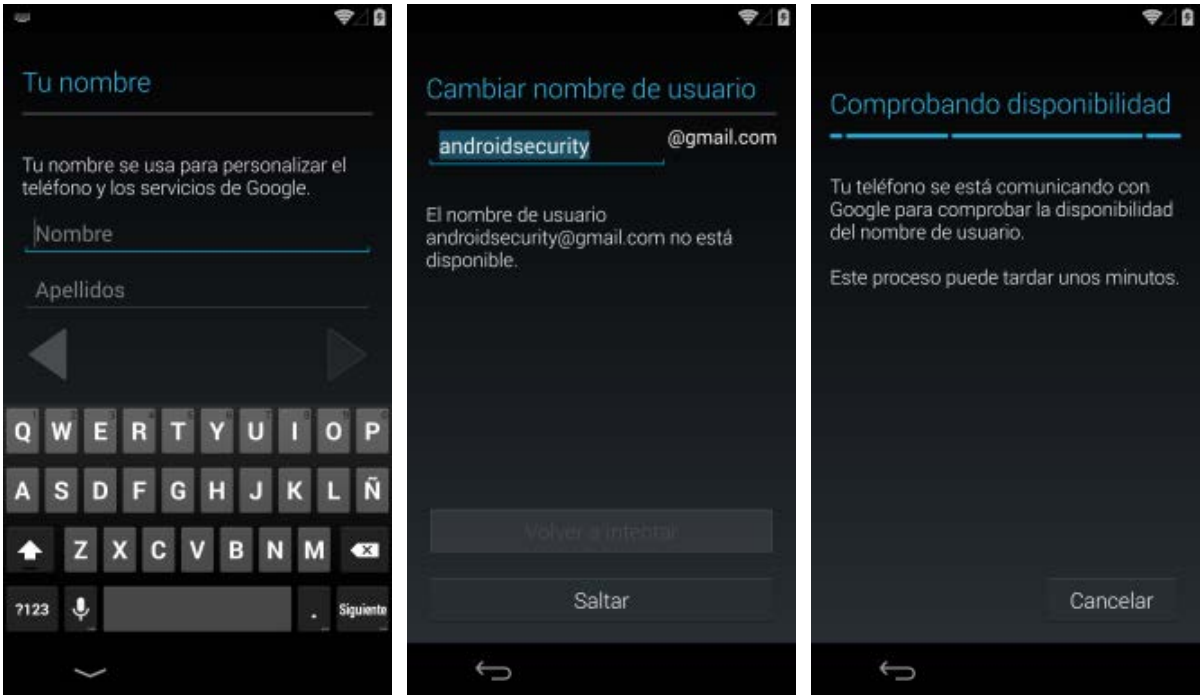
1368. En el caso de seleccionar una red Wi-Fi, establecer una conexión con la misma y obtener conectividad a Internet, se verifica la existencia de la conexión y se ofrece al usuario la posibilidad de configurar su cuenta de usuario de Google en el dispositivo móvil:



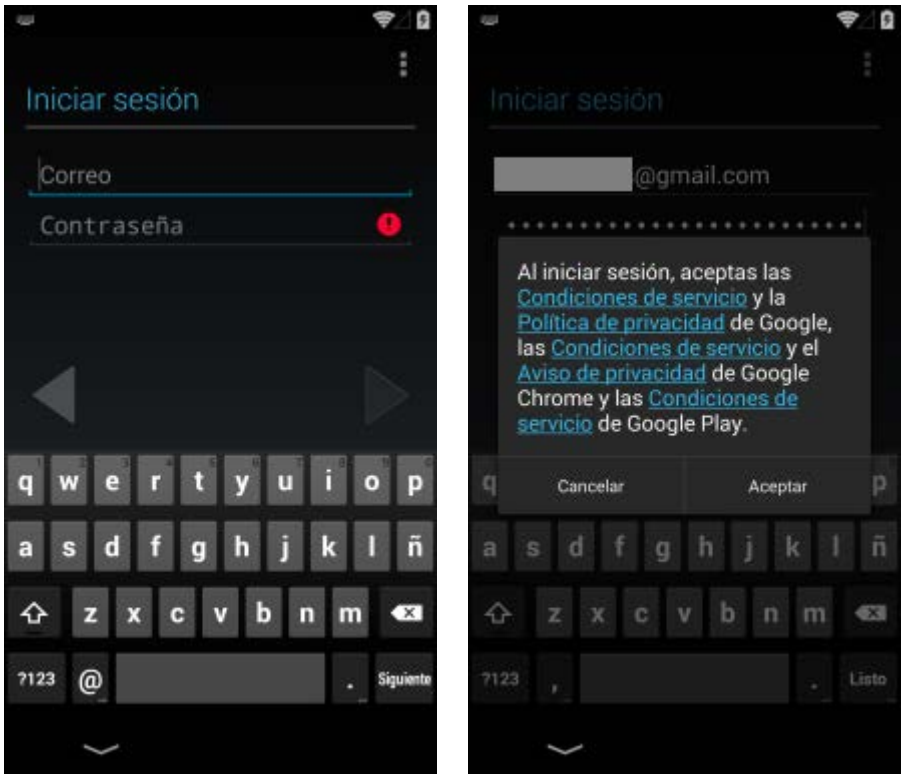
1369. Desde el punto de vista de seguridad se recomienda omitir la vinculación inicial entre el dispositivo móvil y una cuenta de usuario de Google y realizar el proceso de configuración inicial posteriormente, salvo que el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión segura a una red Wi-Fi o 2/3/4G.

1370. Si el usuario no dispone de una cuenta de usuario de Google, se le ofrece la opción de integrar Google en el dispositivo móvil mediante la creación de una cuenta.

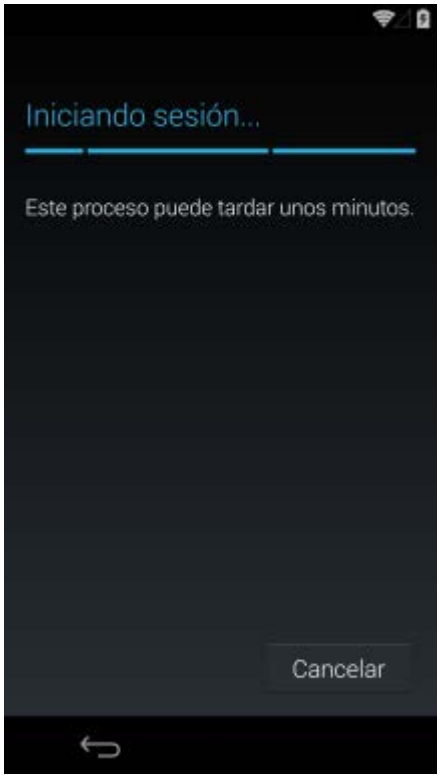
1371. Al crear una cuenta de usuario de Google, se solicita el nombre y apellidos del usuario, y el usuario debe elegir un nombre de usuario en Google, asociado a su cuenta de Gmail (nombredeusuario@gmail.com):



1372. Si ya se dispone de cuenta de usuario de Google, el usuario debe introducir su nombre de usuario en Google, asociado a su cuenta de Gmail (nombredeusuario@gmail.com) y la contraseña asociada, y aceptar las condiciones de servicio y política de privacidad de Google, etc:



1373. Como resultado se inicia sesión con la cuenta de usuario en Google, empleando una conexión cifrada mediante HTTPS, y se le ofrece al usuario la posibilidad de actualizar a Google+ y sus servicios asociados:



1374. En el caso de actualizar a Google+, el usuario debe crear su perfil público asociado, aceptando que Google use su ubicación y aceptando las condiciones de servicio y política de privacidad de Google, etc:

1375. Al asociar el dispositivo móvil a una cuenta de usuario de Google, se debe seleccionar si se quiere hacer uso de los servicios de Google, incluyendo la realización de copias de seguridad y la posibilidad de restauración, y de los servicios de ubicación (las dos opciones

relativas a la ubicación son descritas en detalle posteriormente). Estas tres opciones están habilitadas por defecto:

1376. Adicionalmente, se dispone de una opción en la parte inferior (deshabilitada por defecto) para recibir noticias y ofertas de Google Play.

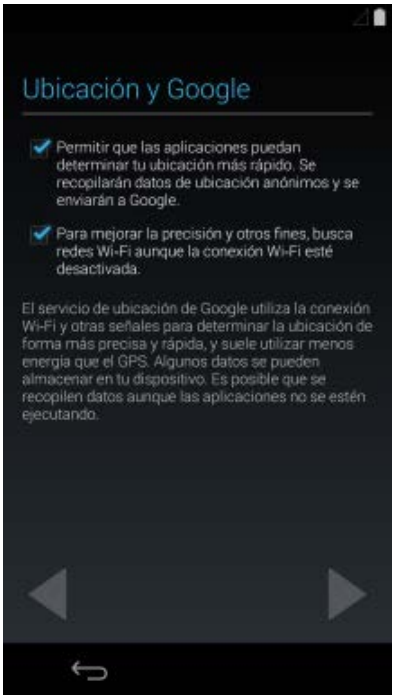
1377. La opción "Copia de seguridad y restauración" habilita las capacidades de Android para hacer una copia de seguridad de los datos del usuario en la cuenta de usuario de Google, incluyendo los datos de las apps, contraseñas de redes Wi-Fi, y otros ajustes de configuración.

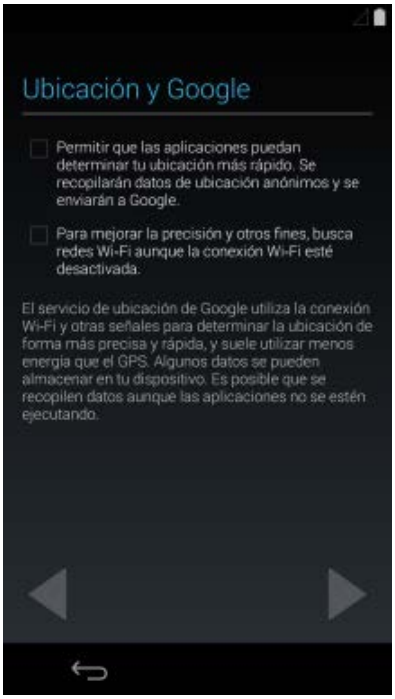
1378. Estas capacidades corresponden con la opción de configuración disponible desde el menú "Ajustes [Personal] - Copia de seguridad". En concreto, todas las opciones serán habilitadas, es decir, se llevará a cabo la copia de datos, y se restaurarán automáticamente la configuración y datos asociados al reinstalar de nuevo una app (ver apartado "5.20. Copias de seguridad").

1379. Desde el punto de vista de seguridad y privacidad, salvo que se disponga de plena confianza en el tratamiento que Google hará de estos datos del usuario, es necesario evaluar en detalle si se desea activar esta funcionalidad.

1380. Adicionalmente, se ofrece al usuario la posibilidad de configurar una tarjeta de crédito para realizar compras en Google Play, asociada al servicio Google Wallet (fuera del alcance del proceso de configuración bajo estudio):

1381. En el caso de no haber vinculado una cuenta de usuario de Google (ni haberse conectado a una red Wi-Fi), la pantalla de "Ubicación y Google" (equivalente a la descrita anteriormente al vincular una cuenta) permite activar ciertas capacidades asociadas a los servicios de ubicación de Google para agilizar la localización del dispositivo por parte de las apps. Las dos opciones (habilitadas por defecto), permiten por un lado recopilar datos de ubicación (teóricamente de redes Wi-Fi y torres de telefonía móvil), supuestamente de forma anónima, que serán enviados a Google, y por otro, hacer uso de las capacidades de búsqueda de redes Wi-Fi para la ubicación, incluso cuando el interfaz Wi-Fi esté deshabilitado:





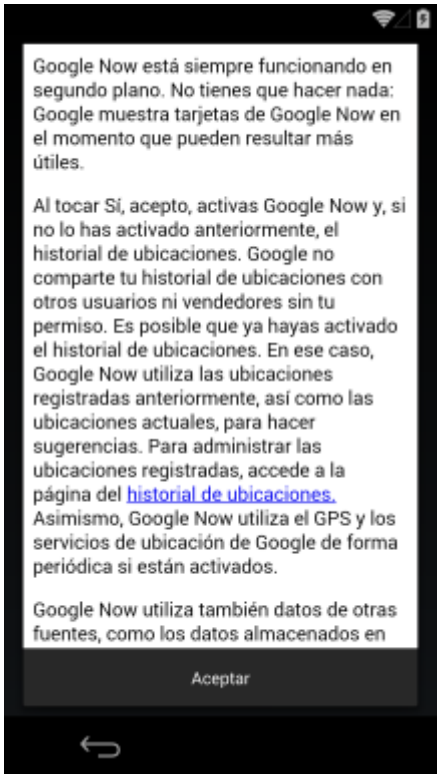
1382. Se recomienda deshabilitar ambas opciones y habilitarlas si se desea posteriormente a través del menú de "Ajustes" correspondiente. En concreto, estas dos opciones corresponden a "Ajustes [Personal] - Ubicación - Modo: Alta precisión" (Determinar ubicación con GPS, Wi-Fi y redes móviles) y a la activación de la opción disponible desde "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre", respectivamente.

1383. En caso de deshabilitar ambas opciones, la configuración de los servicios de ubicación disponible bajo el menú "Ajustes [Personal] - Ubicación - Modo" corresponderá a la opción "Solo en dispositivo".

1384. La pantalla "Fecha y hora" permite establecer los valores de la fecha y hora actuales, y la zona horaria (ej. GMT + 1:00); ver imagen superior derecha.

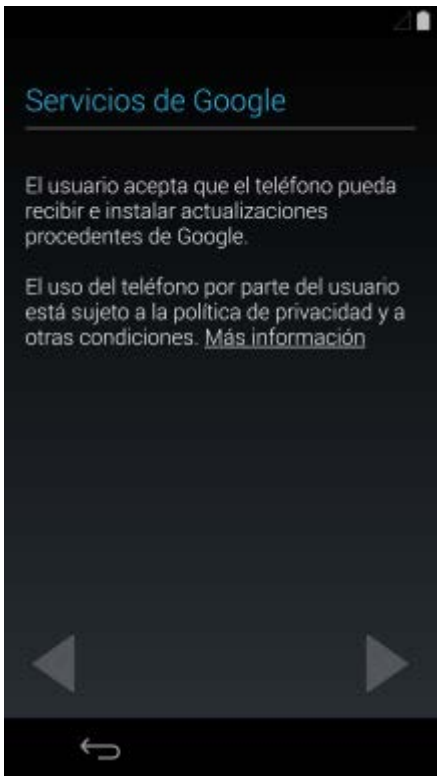
1385. Si se vinculó el dispositivo móvil a una cuenta de usuario de Google, se ofrecen detalles sobre el servicio Google Now, que proporciona información en tiempo real al usuario, y la posibilidad de descargar la app asociada:

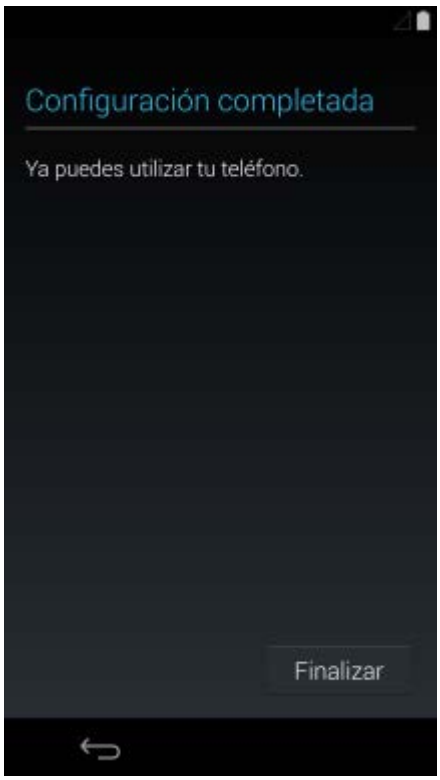
1386. En caso de descargar Google Now, y hacer uso de la misma, se activarán y usarán los servicios de ubicación (aunque previamente se hubieran deshabilitado, incluyendo el historial de ubicaciones - ver apartado "5.10.5. Historial de ubicaciones"), y se accederá a los datos del calendario del usuario, sus búsquedas web (incluyendo el historial web - ver apartado "5.22.1.5. Historial de actividad web") y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros):



1387. Se dispone de más información sobre Google Now en el apartado "5.21. Google Now".

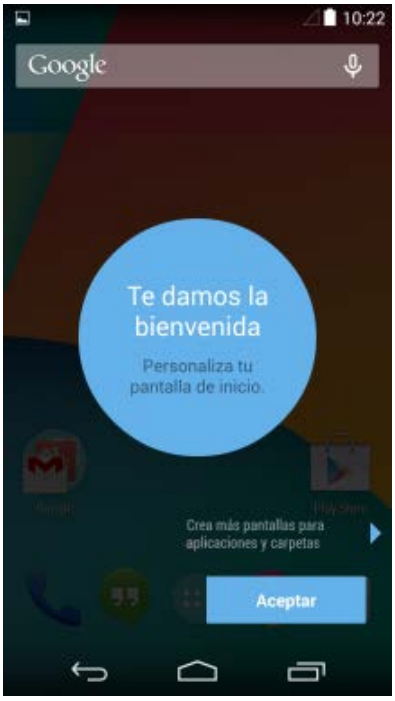
1388. En el caso de no haber vinculado una cuenta de usuario de Google, en lugar de la pantalla de Google Now, a continuación de muestra la pantalla de los "Servicios de Google", que informa sobre la obtención e instalación de actualizaciones, y cuyo uso está sujeto a la política de privacidad y a otras condiciones y términos legales asociados (ver "Más información", con conexión a Internet):





1389. La pantalla final (ver imagen superior derecha) muestra que la configuración ha sido completada con éxito, y el botón "Finalizar" permite empezar a hacer uso del teléfono.

1390. Inicialmente el dispositivo da la bienvenida al usuario y le permite personalizar la pantalla de inicio, guiándole a través de un asistente acerca de cómo llevar a cabo ciertas personalizaciones del interfaz gráfico de usuario (GUI) y de la pantalla de inicio:



1391. Una vez completado el proceso de de instalación y configuración inicial de Android 4.x se recomienda la aplicación de las recomendaciones reflejadas en la presente guía:

7. APÉNDICE B: CAPTURA DE LA PANTALLA EN ANDROID

1392. Por defecto, en versiones previas de Android no existía ninguna aplicación para la captura de la pantalla del dispositivo móvil (*screenshot*). Existían utilidades de terceros que proporcionaban esta funcionalidad pero la mayoría de ellas requerían llevar a cabo el proceso de *rooting* del dispositivo móvil (dependiendo del modelo de dispositivo móvil).

1393. Sin embargo, era posible realizar capturas de la pantalla del dispositivo móvil Android mediante un ordenador a través del puerto USB haciendo uso de las capacidades de depuración del kit de desarrollo de software (SDK, *Software Development Kit*) de Android.

1394. Desde Android 4.0, Ice Cream Sandwich, es posible obtener una captura de la pantalla del dispositivo móvil manteniendo pulsados el botón de encendido/apagado y el botón de bajar el volumen simultáneamente, hasta que se oiga un sonido de confirmación, o se reciba una notificación mediante una animación visual en pantalla.

1395. La captura de pantalla será almacenada en la galería de fotos (o fotografías), dentro de la carpeta "Screenshots", y está disponible a través de USB mediante la carpeta "Pictures/Screenshots" de la memoria interna del dispositivo o de la tarjeta externa de almacenamiento.

1396. Adicionalmente sigue siendo posible realizar una captura de la pantalla del dispositivo mediante ADB (Android Debug Bridge)[118], empleando los siguientes comandos:

```
C:\> adb shell screencap -p /sdcard/screen.png
C:\> adb pull /sdcard/screen.png
C:\> adb shell rm /sdcard/screen.png
```

1397. Por otro lado, desde Android 4.4, KitKat (nivel de API 19), es posible realizar una grabación en vídeo (en formato MPEG-4, sin audio) de la pantalla del dispositivo móvil a través de ADB.

1398. El siguiente comando permite realizar una grabación a 8Mbps de resolución (en lugar de los 4Mbps empleados por defecto), durante 45 segundos (en lugar de emplear la duración por defecto y máxima de 3 minutos, 180 segundos), y almacenará el vídeo en la tarjeta SD del dispositivo móvil:

```
C:\> adb shell screenrecord --bit-rate 8000000 --time-limit 45
/sdcard/kitkat-video.mp4
(Pulsar Ctrl+C para parar la grabación)
```

1399. Se dispone de más información sobre las diferentes opciones de grabación de la pantalla de Android en el sitio web para desarrolladores de Android y, en concreto, de ADB[119].

1400. Si una app muestra vídeos o contenidos protegidos que no desea que sean grabados a través de esta funcionalidad, puede hacer uso del método "SurfaceView.setSecure()" para marcar el contenido como seguro.

[118] http://developer.android.com/tools/help/adb.html
[119] http://developer.android.com/tools/help/adb.html#screenrecord

8. APÉNDICE C: ACTUALIZACIÓN MANUAL COMPLETA A ANDROID 4.4.4

1401. A continuación se muestra, a modo de ejemplo, la salida del script "flash-all" durante el proceso de actualización manual completa a Android versión 4.4.4:

```
C:\FIRMWARE\Nexus5\hammerhead-ktu84p>dir

19/02/2015  16:38    <DIR>          .
19/02/2015  16:38    <DIR>          ..
13/06/2014  18:20         2.568.540 bootloader-hammerhead-hhz11k.img
13/06/2014  18:20               974 flash-all.bat
13/06/2014  18:20               845 flash-all.sh
13/06/2014  18:20               798 flash-base.sh
13/06/2014  18:20       443.843.205 image-hammerhead-ktu84p.zip
13/06/2014  18:20        46.499.328 radio-hammerhead-m8974a-2.0.50.1.16.img
               6 File(s)
               2 Dir(s)

C:\FIRMWARE\Nexus5\hammerhead-ktu84p>flash-all.bat
sending 'bootloader' (2508 KB)...
OKAY [  0.299s]
writing 'bootloader'...
OKAY [  0.499s]
finished. total time: 0.805s
rebooting into bootloader...
OKAY [  0.076s]
finished. total time: 0.081s
sending 'radio' (45409 KB)...
OKAY [  1.641s]
writing 'radio'...
OKAY [  3.110s]
finished. total time: 4.757s
rebooting into bootloader...
OKAY [  0.083s]
finished. total time: 0.086s
archive does not contain 'boot.sig'
archive does not contain 'recovery.sig'
archive does not contain 'system.sig'
archive does not contain 'vendor.img'
Creating filesystem with parameters:
    Size: 13725835264
    Block size: 4096
    Blocks per group: 32768
    Inodes per group: 8144
    Inode size: 256
    Journal blocks: 32768
    Label:
    Blocks: 3351034
    Block groups: 103
    Reserved block group size: 823
Created filesystem with 11/838832 inodes and 93654/3351034 blocks
Creating filesystem with parameters:
    Size: 734003200
    Block size: 4096
    Blocks per group: 32768
    Inodes per group: 7472
    Inode size: 256
    Journal blocks: 2800
```

```
    Label:
    Blocks: 179200
    Block groups: 6
    Reserved block group size: 47
Created filesystem with 11/44832 inodes and 5813/179200 blocks
-----------------------------------------
Bootloader Version...: HHZ11k
Baseband Version.....: M8974A-2.0.50.1.16
Serial Number........: 0938c7dd02814740
-----------------------------------------
checking product...
OKAY [  0.100s]
checking version-bootloader...
OKAY [  0.097s]
checking version-baseband...
OKAY [  0.098s]
sending 'boot' (8700 KB)...
OKAY [  0.498s]
writing 'boot'...
OKAY [  0.740s]
sending 'recovery' (9284 KB)...
OKAY [  0.553s]
writing 'recovery'...
OKAY [  0.774s]
erasing 'system'...
OKAY [  1.092s]
sending 'system' (721400 KB)...
OKAY [ 24.361s]
writing 'system'...
OKAY [ 49.161s]
erasing 'userdata'...
OKAY [  8.886s]
sending 'userdata' (137318 KB)...
OKAY [  4.690s]
writing 'userdata'...
OKAY [  9.149s]
erasing 'cache'...
OKAY [  0.669s]
sending 'cache' (13348 KB)...
OKAY [  0.647s]
writing 'cache'...
OKAY [  1.069s]
rebooting...

finished. total time: 103.119s
Press any key to exit...
```

1402. Tras unos minutos, el dispositivo móvil arrancará con la nueva versión de Android y comenzará el proceso de instalación y configuración inicial (ver apartado "6. Apéndice A: Proceso de instalación y configuración inicial").

9. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	"Guía CCN-STIC-450: Seguridad de dispositivos móviles". CCN-CERT. Mayo 2013. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/ 450-Seguridad_Dispositivos_Móviles/450_SEGURIDAD_EN_DISPOSITIV.PDF
[Ref.- 2]	Android. Google. URL: http://www.android.com
[Ref.- 3]	Google Nexus 5. Google. URL: http://www.google.com/nexus/5/
[Ref.- 4]	Google Play. URL: https://play.google.com
[Ref.- 5]	"Exercising Our Remote Application Removal Feature". Rich Cannings. Android. June 2010. URL: http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html
[Ref.- 6]	"An Update on Google Play Security". Google. March 2011. URL: http://googlemobile.blogspot.com/2011/03/update-on-android-Play-security.html
[Ref.- 7]	Android Developers. Google. URL: http://developer.android.com
[Ref.- 8]	"The dark side of the new Google Play". Denis. Kaspersky Lab Expert. February 2011. URL:http://www.securelist.com/en/blog/11153/The_dark_side_of_the_new_Android_Play
[Ref.- 9]	"Android 2.3 Platform and Updated SDK Tools". December 2010. Google. URL: http://android-developers.blogspot.com/2010/12/android-23-platform-and-updated-sdk.html
[Ref.- 10]	"Android 2.3.3 Platform, New NFC Capabilities". February 2011. Google. URL:http://android-developers.blogspot.com/2011/02/android-233-platform-new-nfc.html
[Ref.- 11]	"Android - About Google. URL: http://developer.android.com/about/index.html
[Ref.- 12]	"Bring Your Phone to Work Day: Managing Android Devices With Google Apps". October 2010. Google. URL: http://googleenterprise.blogspot.com/2010/10/bring-your-phone-to-work-day-managing.html
[Ref.- 13]	"Google Apps Device Policy". Google. URL: https://market.android.com/details?id=com.google.android.apps.enterprise.dmagent URL: https://www.google.com/support/mobile/bin/answer.py?hl=en&answer=190930
[Ref.- 14]	"Google Authenticator". Google. Play Store. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2 URL: https://www.google.com/support/accounts/bin/answer.py?answer=1066447
[Ref.- 15]	"About 2-step verification". Google. URL: https://support.google.com/accounts/answer/180744
[Ref.- 16]	"Application Fundamentals". Android Developers. Google. URL: http://developer.android.com/guide/components/fundamentals.html
[Ref.- 17]	"Security and Permissions". Android Developers. Google. URL: http://developer.android.com/guide/topics/security/security.html
[Ref.- 18]	"Mobile Application Security". Himanshu Dwivedi, Chris Clark, David Thiel. McGraw-Hill. ISBN: 0071633561. 2010. URL: http://www.mhprofessional.com/product.php?isbn=0071633561
[Ref.- 19]	"API Levels". Android Developers. Google. URL: http://developer.android.com/guide/appendix/api-levels.html
[Ref.- 20]	"Verificación en dos pasos (two-step verification)". Google. URL: https://www.google.com/landing/2step/ URL: https://www.google.com/landing/2step/features.html
[Ref.- 21]	"Android VPN Connectivity". pfSense. URL: https://doc.pfsense.org/index.php/Android_VPN_Connectivity
[Ref.- 22]	Android Studio & SDK (Software Development Kit). Google. URL: http://developer.android.com/sdk/index.html

Referencia	Título, autor y ubicación
[Ref.- 23]	Manifest Permission (Since API Level 1). Google. URL: http://developer.android.com/reference/android/Manifest.permission.html
[Ref.- 24]	"Android Quick Start Guide, Android 4.4 (KitKat)". Google. 2013. URL: https://play.google.com/store/books/details/Google_Inc_Android_Quick_Start_Guide_Android_4_4_K?id=3SfNAQAAQBAJ (US EN) ; URL: https://play.google.com/store/books/details/Google_Inc_Android_Quick_Start_Guide_Android_Mobil?id=9rrqAgAAQBAJ (UK EN)
[Ref.- 25]	"Android: Guía de inicio rápido, Android 4.4 (KitKat)". Google. 2013.URL: https://play.google.com/store/books/details/Google_Inc_Gu%C3%ADa_de_inicio_r%C3%A1pido_Plataforma_de_tec?id=JvDqAgAAQBAJ
[Ref.- 26]	"Code signing in Android's security model". Nikolay Elenkov. May 2013. URL: http://nelenkov.blogspot.com.es/2013/05/code-signing-in-androids-security-model.html
[Ref.- 27]	"BouncyCastle Key Store (BKS) library". The Legion of the Bouncy Castle. URL: http://bouncycastle.org/download/bcprov-jdk16-141.jar
[Ref.- 28]	"Signing Your Applications". Android Developers. URL: http://developer.android.com/guide/publishing/app-signing.html
[Ref.- 29]	RedPhone. Open WhisperSystems. 2015. URL: https://whispersystems.org URL: https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
[Ref.- 30]	"Getting Your SMS Apps Ready for KitKat". Android Developers Blog. October 2013. URL: http://android-developers.blogspot.com.es/2013/10/getting-your-sms-apps-ready-for-kitkat.html
[Ref.- 31]	"Android 3.0 Platform Highlights". Google. 2011. URL: http://developer.android.com/sdk/android-3.0-highlights.html#enterprise
[Ref.- 32]	Wickr. 2015. URL: https://wickr.com URL: https://play.google.com/store/apps/details?id=com.mywickr.wickr2
[Ref.- 33]	TextSecure. Open WhisperSystems. 2015. URL: https://whispersystems.org URL: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
[Ref.- 34]	"Android 2.2 Platform Highlights". Google. 2010. URL: http://developer.android.com/sdk/android-2.2-highlights.html
[Ref.- 35]	"Perform a Remote Wipe on a Mobile Phone" (MS Exchange 2010). Microsoft Technet. 2009. URL: http://technet.microsoft.com/en-us/library/aa998614.aspx
[Ref.- 36]	"Understanding Exchange ActiveSync Mailbox Policies·. MS Exchange 2010 SP2 & SP3. Microsoft Technet. 2014. URL: https://technet.microsoft.com/en-us/library/bb123484.aspx
[Ref.- 37]	"View or Configure Exchange ActiveSync Mailbox Policy Properties" (Microsoft Exchange 2010). Microsoft Technet. 2010. URL: http://technet.microsoft.com/en-us/library/bb123994.aspx
[Ref.- 38]	"Android support for Microsoft Exchange in pure Google devices". Google. 2013. URL: http://static.googleusercontent.com/media/www.google.com/es//help/hc/images/android/MicrosoftExchangePoliciesinAndroid.pdf
[Ref.- 39]	"Administrador de dispositivos Android". Google. URL: https://support.google.com/accounts/answer/3265955?hl=es
[Ref.- 40]	"Issue 82: wifi - support ad hoc networking". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=82
[Ref.- 41]	"Ad-Hoc (IBSS) mode support for Android 4.2.2 / 4.3 / 4.4". Thinktube. March 2014. URL: http://www.thinktube.com/tech-en/android/wifi-ibss
[Ref.- 42]	"Why Wi-Fi Direct cannot replace Ad-hoc mode". szym. Thinktube. 2014. URL: http://www.thinktube.com/tech-en/android/wifi-direct
[Ref.- 43]	"Issue 1041: Hidden SSID Fails to Connect". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=1041
[Ref.- 44]	"How can I trust CAcert's root certificate?". CAcert Wiki. URL: http://wiki.cacert.org/ImportRootCert#Android_Phones
[Ref.- 45]	"Android code signing". Nikolay Elenkov. April 2013. URL: http://nelenkov.blogspot.com.es/2013/04/android-code-signing.html

Referencia	Título, autor y ubicación
[Ref.- 46]	"RealmB's Android Certificate Installer". RealmB. URL: http://www.realmb.com/droidCert/
[Ref.- 47]	Settings-Secure. Android Developers. URL: http://developer.android.com/reference/android/provider/Settings.Secure.html
[Ref.- 48]	dhcpcd. Roy Marples. URL: http://roy.marples.name/projects/dhcpcd/index
[Ref.- 49]	"Guía CCN-STIC-406: Seguridad en redes inalámbricas". CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 50]	"Description of the Wireless Client Update for Windows XP with Service Pack 2". Microsoft. 2010. URL: http://support.microsoft.com/kb/917021
[Ref.- 51]	"Guía CCN-STIC-418: Seguridad en Bluetooth". CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 52]	"ConnectivityManager". Android Developers. URL: http://developer.android.com/reference/android/net/ConnectivityManager.html
[Ref.- 53]	"Wi-Fi Direct ("P2P")". Wi-Fi Alliance. 2013. URL: http://www.wi-fi.org/discover-and-learn/wi-fi-direct
[Ref.- 54]	"Issue 3389: Full IPv6 Android support". Android Google Code. 2009. URL: https://code.google.com/p/android/issues/detail?id=3389 URL: https://code.google.com/p/android/issues/detail?id=3389#c107
[Ref.- 55]	"Issue 14013: Enable IPv6 Privacy Extensions". Android Google Code. 2011. URL: https://code.google.com/p/android/issues/detail?id=14013 URL: http://www.h-online.com/security/news/item/IPv6-Smartphones-compromise-users-privacy-1169708.html
[Ref.- 56]	"These aren't the permissions you're looking for". A. Lineberry, D. Richardson, T. Wyatt". Defcon 18. 2010. URL: http://www.defcon.org/images/defcon-18/dc-18-presentations/Lineberry/DEFCON-18-Lineberry-Not-The-Permissions-You-Are-Looking-For.pdf
[Ref.- 57]	"Support connecting to IPv6-only wireless networks". Android Google Code. June 2012. URL: https://code.google.com/p/android/issues/detail?id=32630
[Ref.- 58]	"Android 4.4.4 OTA rollout to Nexus devices begins". Android Central. Junio 2014. URL: http://www.androidcentral.com/android-444-ota-rollout-begins
[Ref.- 59]	"Use of IPv6 privacy extensions should be configurable ". Android Google Code. May 2012. URL: https://code.google.com/p/android/issues/detail?id=31102
[Ref.- 60]	"2 big points critics always miss about Android upgrades". Computer World. June 2015. URL: http://www.computerworld.com/article/2476391/android/2-big-points-critics-always-miss-about-android-upgrades.html
[Ref.- 61]	"Cómo administrar mis dispositivos". Google. URL: https://support.google.com/a/users/answer/1235372?hl=es
[Ref.- 62]	"12 Days of HaXmas: A year of Metasploit Android exploits". Rapid 7. January 2015. URL: https://community.rapid7.com/community/metasploit/blog/2015/01/02/2014-a-year-of-android-exploits-in-metasploit
[Ref.- 63]	"WebView addJavascriptInterface Remote Code Execution". MRW Labs. September 2013. URL: https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/ URL: https://labs.mwrinfosecurity.com/blog/2012/04/23/adventures-with-android-webviews/
[Ref.- 64]	"Por qué se debe iniciar sesión en Chrome". Google. URL: https://support.google.com/chrome/answer/165139?hl=es URL: https://support.google.com/chrome/answer/1181035 URL: https://support.google.com/chrome/answer/2591582?hl=es
[Ref.- 65]	Android Vulnerabilities. 2015. URL: http://androidvulnerabilities.org
[Ref.- 66]	"No puedes desbloquear el dispositivo Android". Google. URL: https://support.google.com/nexus/answer/3388218?hl=es
[Ref.- 67]	"Android Security Announcements". Google Groups. 2008. URL: https://groups.google.com/group/android-security-announce
[Ref.- 68]	"Android Security Discussions". Google Groups. 2008. URL: http://groups.google.com/group/android-security-discuss
[Ref.- 69]	"Android Security FAQ". Android Developers. URL: http://developer.android.com/resources/faq/security.html

Referencia	Título, autor y ubicación
[Ref.- 70]	"Google Play Devices". Google. URL: https://play.google.com/store/devices
[Ref.- 71]	"Google Experience Devices". DanKor. 2012. URL: http://about.me/googleexperiencedevice URL: http://googleexperiencedevice.blogspot.com
[Ref.- 72]	"Factory Images for Nexus Devices". Google. URL: https://developers.google.com/android/nexus/images
[Ref.- 73]	"Android WiFi-Direct Denial of Service". Core Security. January 2015. URL: http://www.coresecurity.com/advisories/android-wifi-direct-denial-service
[Ref.- 74]	"Android Screen Lock Bypass". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/ URL: https://play.google.com/store/apps/details?id=net.thomascannon.screenlockbypass.pro
[Ref.- 75]	"Android Market Security". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-market-security/
[Ref.- 76]	"Certificate pinning in Android 4.2". Nikolay Elenkov. December 2012. URL: http://nelenkov.blogspot.com/2012/12/certificate-pinning-in-android-42.html
[Ref.- 77]	"A Peek Inside the GTalkService Connection". Jon Oberheide. 2010. URL: http://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/
[Ref.- 78]	"Remote Kill and Install on Google Android". Jon Oberheide. 2010. URL: http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/
[Ref.- 79]	"Apple. Google Collect User Data". Wall Street Journal. 2011. URL: http://on.wsj.com/gDfmEV
[Ref.- 80]	"Android Map". Samy Kamkar. 2011. URL: http://samy.pl/androidmap/
[Ref.- 81]	Android Open Source Project (AOSP). URL: http://source.android.com
[Ref.- 82]	"Notes on the implementation of encryption in Android 3.0". AOSP. URL: http://source.android.com/tech/encryption/android_crypto_implementation.html
[Ref.- 83]	"Android X.Y Platform Highlights" & "Welcome to Android 4.x". Android Developers. URL (2.2): http://developer.android.com/about/versions/android-2.2-highlights.html URL (2.3): http://developer.android.com/about/versions/android-2.3-highlights.html URL (3.0): http://developer.android.com/about/versions/android-3.0-highlights.html URL (4.0): http://developer.android.com/about/versions/android-4.0-highlights.html URL (4.1): http://developer.android.com/about/versions/jelly-bean.html#android-41 URL (4.2): http://developer.android.com/about/versions/jelly-bean.html#android-42 URL (4.3): http://developer.android.com/about/versions/jelly-bean.html#android-43 URL (4.4): http://developer.android.com/about/versions/kitkat.html URL (5.0): http://developer.android.com/about/versions/lollipop.html
[Ref.- 84]	"Android 2.2 Platform - Revisions". Android Developers. URL: http://developer.android.com/sdk/android-2.2.html
[Ref.- 85]	"Inside the Android Security Patch Lifecycle". Tim Wyatt. Lookout. August 2011. URL: http://blog.mylookout.com/blog/2011/08/04/inside-the-android-security-patch-lifecycle/
[Ref.- 86]	CTS (Compatibility Test Suite). AOSP. URL: http://source.android.com/compatibility/cts-intro.html
[Ref.- 87]	"Researcher Builds Mock Botnet Of 'Twilight'-Loving Android Users". Forbes. Junio 2010. URL: http://www.forbes.com/sites/firewall/2010/06/21/researcher-builds-mock-botnet-of-twilight-loving-android-users/
[Ref.- 88]	"Device Policy for Android" & "Device Policy Administration for Android" & "Google Apps Mobile Management: Overview". Google Mobile. URL: https://support.google.com/mobile/bin/answer.py?hl=en&answer=190930 URL: http://support.google.com/a/bin/answer.py?hl=en&answer=1056433 URL: https://support.google.com/a/bin/answer.py?hl=en&answer=1734200
[Ref.- 89]	"Issue 6111: Allow a hostname to be specified". Android Google Code. January 2010. URL: https://code.google.com/p/android/issues/detail?id=6111
[Ref.- 90]	"Unpacking Android backups". Nikolay Elenkov. June 2012. URL: http://nelenkov.blogspot.com.es/2012/06/unpacking-android-backups.html URL: https://github.com/nelenkov/android-backup-extractor

Referencia	Título, autor y ubicación
[Ref.- 91]	"Anclaje a red y zona Wi-Fi". Google Mobile. URL: https://support.google.com/nexus/answer/2812516?hl=es
[Ref.- 92]	"[TAD-2011-003] Vulnerability in Android: To add, or not to add (a Wi-Fi network), that is the question". Raul Siles. Taddong. Mayo 2010. URL: http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html
[Ref.- 93]	"Issue 1215: IP settings for WiFi networks". Android Android Google Code. November 2008. URL: https://code.google.com/p/android/issues/detail?id=1215
[Ref.- 94]	"Putting Android to work for your business". Official Google Enterprise Blog. April 2011. URL: http://googleenterprise.blogspot.com/2011/04/putting-android-to-work-for-your.html
[Ref.- 95]	"Update the Galaxy Nexus with Android 4.4 "KitKat"". Change.org. October 2013. URL: https://www.change.org/p/google-update-the-galaxy-nexus-with-android-4-4-kitkat
[Ref.- 96]	"Issue 11855: Support settings change in Android WIFI/USB Tether". Android Google Code. October 2010. URL: https://code.google.com/p/android/issues/detail?id=11855
[Ref.- 97]	"A Tale Of Another SOP Bypass In Android Browser < 4.4". Rafay Baloch . October 2014. URL: http://www.rafayhackingarticles.net/2014/10/a-tale-of-another-sop-bypass-in-android.html URL: https://community.rapid7.com/community/metasploit/blog/2014/11/06/metasploit-weekly-wrapup
[Ref.- 98]	"Android Fake ID Vulnerability Lets Malware Impersonate Trusted Applications, Puts All Android Users Since January 2010 At Risk". BlueBox. July 2014. URL: https://bluebox.com/blog/technical/android-fake-id-vulnerability/
[Ref.- 99]	"Package javax.net.ssl". Android Developers. URL: http://developer.android.com/reference/javax/net/ssl/package-summary.html
[Ref.- 100]	"Official Ice Cream Sandwich for the Nexus One won't happen, Google says". Android Central. October 2011. URL: http://www.androidcentral.com/official-ice-cream-sandwich-nexus-one-wont-happen-google-says
[Ref.- 101]	"Copia de seguridad y restauración de datos del dispositivo". Google. URL: https://support.google.com/nexus/answer/2819582?hl=es
[Ref.- 102]	"The AndroidManifest.xml File: <permission>". Android Developers. URL: http://developer.android.com/guide/topics/manifest/permission-element.html#plevel
[Ref.- 103]	"SE Android". SE Linux Project. 2012. URL: http://selinuxproject.org/page/SEAndroid URL: http://selinuxproject.org/~jmorris/lss2011_slides/caseforseandroid.pdf
[Ref.- 104]	"Clasificaciones de contenido de las aplicaciones". Google Play. URL: http://support.google.com/androidPlay/bin/answer.py?hl=es&answer=1075738
[Ref.- 105]	"Flash to Focus on PC Browsing and Mobile Apps; Adobe to More Aggressively Contribute to HTML5". Adobe. Noviembre 2011. URL: http://blogs.adobe.com/conversations/2011/11/flash-focus.html
[Ref.- 106]	"Issue 10809: Password is stored on disk in plain text". Android Google Code. August 2010. URL: https://code.google.com/p/android/issues/detail?id=10809
[Ref.- 107]	"Android Debug Bridge (ADB)". Android Developers. URL: http://developer.android.com/guide/developing/tools/adb.html
[Ref.- 108]	"Catching AuthTokens in the Wild - The Insecurity of Google's ClientLogin Protocol". Bastian Könings, Jens Nickels, and Florian Schaub. Mayo 2011. URL: http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html URL: https://freedom-to-tinker.com/blog/dwallach/things-overheard-wifi-my-android-smartphone URL: http://android.stackexchange.com/questions/3129/what-android-syncd-data-is-encrypted
[Ref.- 109]	"Chrome for Android". Google. URL: https://developer.chrome.com/multidevice/faq
[Ref.- 110]	"Google Data Protocol - FAQ". Google Code. URL: https://code.google.com/apis/gdata/faq.html#clientlogin_expire
[Ref.- 111]	"Authentication and Authorization for Google APIs - ClientLogin for Installed Applications". Google Code. URL: https://code.google.com/apis/accounts/docs/AuthForInstalledApps.html
[Ref.- 112]	"Using OAuth 2.0 to Access Google APIs". Google. URL: https://developers.google.com/accounts/docs/OAuth2

Referencia	Título, autor y ubicación
[Ref.- 113]	"LOOK-10-007 – TapJacking". Lookout. December 2010. URL: http://blog.mylookout.com/look-10-007-tapjacking/ URL: http://blog.mylookout.com/blog/2010/12/09/android-touch-event-hijacking/
[Ref.- 114]	"Android Master Key Exploit – Uncovering Android Master Key That Makes 99% of Devices Vulnerable". BlueBox. July 2013. URL: https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/
[Ref.- 115]	"Android Browser Same Origin Policy Bypass < 4.4 - CVE-2014-6041". Rafay Baloch . September 2014. URL: http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html URL: https://community.rapid7.com/community/metasploit/blog/2014/09/15/major-android-bug-is-a-privacy-disaster-cve-2014-6041
[Ref.- 116]	"Android WebView fixes". Adrian Ludwig. January 2015. URL: https://plus.google.com/+AdrianLudwig/posts/1md7ruEwBLF URL: https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior URL: https://community.rapid7.com/community/metasploit/blog/2015/01/16/weekly-metasploit-wrapup
[Ref.- 117]	"Issue 8196: Enhancement: Client Certificate Authentication in Browser". Android Google Code. May 2010. URL: https://code.google.com/p/android/issues/detail?id=8196
[Ref.- 118]	"Issue 11231: Provide support for managing CA and client certificates". Android Google Code. September 2010. URL: https://code.google.com/p/android/issues/detail?id=11231
[Ref.- 119]	"KeyChain". Android Developers. URL: http://developer.android.com/reference/android/security/KeyChain.html
[Ref.- 120]	"Firmware" & "Release History". Shawn. Random Phantasmagoria. URL: http://www.randomphantasmagoria.com/firmware/ URL: http://www.randomphantasmagoria.com/release-history/
[Ref.- 121]	"Browser Security Handbook, part 2". Michal Zalewski. Marzo 2011 (actualizado). URL: https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
[Ref.- 122]	"Android Reference Devices Through the Years". Shawn. Random Phantasmagoria. October 2013. URL: http://www.randomphantasmagoria.com/android-reference-devices-through-the-years/
[Ref.- 123]	"Issue 6348: Bluetooth should have the option to be constantly discoverable and not just have a set time limit". Android Google Code. January 2010. URL: https://code.google.com/p/android/issues/detail?id=6348
[Ref.- 124]	"Malicious Android Applications: Risks and Exploitation". Joany Boutet. SANS Reading Room. Marzo 2010. URL: https://www.sans.org/reading_room/whitepapers/malicious/malicious-android-applications-risks-exploitation_33578
[Ref.- 125]	"App Ops Brings Granular Permissions Control to Android 4.3". Will Verduzco. Julio 2013. URL: http://www.xda-developers.com/app-ops-brings-granular-permissions-control-to-android-4-3/ URL: http://www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-app-permission-manager-control-permissions-for-individual-apps/
[Ref.- 126]	"App Ops Lives On In Android 4.4, Can Now Deny Even More Permissions". Android Police. November 2013. URL: http://www.androidpolice.com/2013/11/25/new-app-app-ops-lives-on-in-android-4-4-can-be-unleashed-with-app-ops-from-color-tiger-and-enhanced-with-root/
[Ref.- 127]	"Using WebView - Security Tips". Google. 2015. URL: http://developer.android.com/training/articles/security-tips.html#WebView
[Ref.- 128]	"Android Version History". Wikipedia. URL: https://en.wikipedia.org/wiki/Android_version_history
[Ref.- 129]	"AppOps". Sylvain Galand. URL: https://play.google.com/store/apps/details?id=fr.slvn.appops&hl=en URL: https://github.com/slvn/android-appops-launcher

Referencia	Título, autor y ubicación
[Ref.- 130]	"Guía CCN-STIC-453 - Seguridad de dispositivos móviles: Android". CCN-CERT. Mayo 2013. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/ 453-Seguridad_Android/453SeguridadenAndroidmay13.pdf
[Ref.- 131]	"CCN-STIC-457: Gestión de dispositivos móviles: MDM (Mobile Device Management)". CCN-CERT. Noviembre 2013. URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/457/457-Gestion_dispositivos_móviles_MDM-nov13.pdf
[Ref.- 132]	"Revisiting Android disk encryption". Nikolay Elenkov. Octubre 2014. URL: http://nelenkov.blogspot.com.es/2014/10/revisiting-android-disk-encryption.html
[Ref.- 133]	"DevBytes: Android L Developer Preview". Google Developers. Julio 2014. URL: https://www.youtube.com/watch?v=s7JLYYkJuNs#t=90
[Ref.- 134]	"Introducing Android 4.3, a sweeter Jelly Bean". Official Android Blog. Julio 2013. URL: http://officialandroid.blogspot.com.es/2013/07/introducing-android-43-sweeter-jelly.html
[Ref.- 135]	"DevBytes: Restricted Profiles in Android 4.3". Google Developers. Julio 2014. URL: https://www.youtube.com/watch?v=pdUcANNm72o
[Ref.- 136]	"CCS Injection Vulnerability". Lepidum. June 2014. URL: http://ccsinjection.lepidum.co.jp URL: http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html
[Ref.- 137]	"Early ChangeCipherSpec Attack". Imperial Violet - Adam Langley. Junio 2014. URL: https://www.imperialviolet.org/2014/06/05/earlyccs.html
[Ref.- 138]	"Security Enhancements in Android 4.x (o 5.x)". Android Source. URL: https://source.android.com/devices/tech/security/enhancements42.html URL: https://source.android.com/devices/tech/security/enhancements43.html URL: https://source.android.com/devices/tech/security/enhancements44.html URL: https://source.android.com/devices/tech/security/enhancements50.html
[Ref.- 139]	"Android Hacker's Handbook". Wiley. 2014.
[Ref.- 140]	"Security-Enhanced Linux in Android". Android Source. URL: http://source.android.com/devices/tech/security/se-linux.html
[Ref.- 141]	Google Cloud Messaging (GCM) for Android. Google. URL: http://developer.android.com/google/gcm/index.html
[Ref.- 142]	"Credential storage enhancements in Android 4.3". Nikolay Elenkov. August 2013. URL: http://nelenkov.blogspot.com.es/2013/08/credential-storage-enhancements-android-43.html
[Ref.- 143]	"Android KeyStore Stack Buffer Overflow". CVE-2014-3100. June 2014. URL: http://www.exploit-db.com/wp-content/themes/exploit/docs/33864.pdf
[Ref.- 144]	"Secure USB debugging in Android 4.2.2". Nikolay Elenkov. Febrero 2013. URL: http://nelenkov.blogspot.com.es/2013/02/secure-usb-debugging-in-android-422.html URL: http://android-developers.blogspot.jp/2013/02/security-enhancements-in-jelly-bean.html
[Ref.- 145]	"Utilizar el identificador de llamada de Google". Google. 2014. URL: https://support.google.com/nexus/answer/3459196?hl=es
[Ref.- 146]	"Android 4.4 - KitKat". Google. URL: http://www.android.com/versions/kit-kat-4-4/ URL: https://www.youtube.com/watch?v=sONcojECWXs
[Ref.- 147]	"Administrar la ubicación de tu dispositivo". Google. URL: https://support.google.com/nexus/answer/3467281?hl=es
[Ref.- 148]	Google Play Services. Google. URL: https://developer.android.com/google/play-services/index.html
[Ref.- 149]	"On the WebView addJavascriptInterface Saga". DroidSec. February 2014. URL: http://www.droidsec.org/news/2014/02/26/on-the-webview-addjsif-saga.html
[Ref.- 150]	"Updating Your Security Provider to Protect Against SSL Exploits". Android. URL: http://developer.android.com/training/articles/security-gms-provider.html
[Ref.- 151]	"Issue 52314: unlock password is limited to 16 characters". Android Google Code. February 2013. URL: https://code.google.com/p/android/issues/detail?id=52314
[Ref.- 152]	"Issue 29468: Different passwords for encryption and screen lock". Android Google Code. April 2012. URL: https://code.google.com/p/android/issues/detail?id=29468

Referencia	Título, autor y ubicación
[Ref.- 153]	"EncPassChanger". Kibab. December 2012. URL: https://github.com/kibab/encpasschanger URL: https://play.google.com/store/apps/details?id=com.kibab.android.EncPassChanger
[Ref.- 154]	"Cryptfs Password". Nikolay Elenkov. August 2013. URL: https://play.google.com/store/apps/details?id=org.nick.cryptfs.passwdmanager URL: https://github.com/nelenkov/cryptfs-password-manager
[Ref.- 155]	"Changing Android's disk encryption password". Nikolay Elenkov. August 2012. URL: http://nelenkov.blogspot.com/2012/08/changing-androids-disk-encryption.html
[Ref.- 156]	"Android encryption switched to scrypt in 4.4.2". AOSP. URL: https://android.googlesource.com/platform/system/vold/+/android-4.4_r1/cryptfs.c URL: https://android.googlesource.com/platform/system/vold/+log/android-4.4_r1/cryptfs.c (commit c4c70f1) URL: https://android.googlesource.com/platform/system/vold/+/c4c70f15bb8845b02f9ec1d624794757badd6933
[Ref.- 157]	"Android Security Internals". Nikolay Elenkov. No Starch Press. October 2014. URL: http://www.nostarch.com/androidsecurity
[Ref.- 158]	"Android's Permissions System Is Broken and Google Just Made It Worse". Chris Hoffman. December 2013. URL: http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/
[Ref.- 159]	"Android's App Permissions Were Just Simplified - Now They're Much Less Secure". Chris Hoffman. June 2014. URL: http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/
[Ref.- 160]	"Revisar los permisos la aplicación". Google. 2014. URL: https://support.google.com/googleplay/answer/6014972?hl=es
[Ref.- 161]	"Utilizar widgets en la pantalla de bloqueo". Google. URL: https://support.google.com/nexus/answer/2781801?hl=es
[Ref.- 162]	"Storage Access Framework". Google. URL: https://developer.android.com/guide/topics/providers/document-provider.html URL: https://www.youtube.com/watch?v=zxHVeXbK1P4 URL: https://www.youtube.com/watch?v=UFj9AEz0DHQ
[Ref.- 163]	"Activar o desactivar SafeSearch". Google. URL: https://support.google.com/websearch/answer/510?hl=es
[Ref.- 164]	"Ubicación en Ajustes de Google". Google. URL: https://support.google.com/accounts/answer/3118687?hl=es
[Ref.- 165]	"ART (Android RunTime)". Google. URL: http://source.android.com/devices/tech/dalvik/
[Ref.- 166]	"Android and Security" (Google Bouncer). Google Mobile Blog. February 2012. URL: http://googlemobile.blogspot.com/2012/02/android-and-security.html
[Ref.- 167]	"Android 4.2 'Verify apps' security feature explained by Google". Android Authority. November 2012. URL: http://www.androidauthority.com/android-4-2-verify-apps-security-feature-explained-by-google-131514/
[Ref.- 168]	"Expanding Google's security services for Android". Android Official Blog. April 2014. URL: http://officialandroid.blogspot.com.es/2014/04/expanding-googles-security-services-for.html
[Ref.- 169]	"Protegerse frente a aplicaciones dañinas". Google. URL: https://support.google.com/accounts/answer/2812853?hl=es URL: https://plus.google.com/+MichaelMorrissey/posts/dutcnbu72pv
[Ref.- 170]	"An Evaluation of the Application ("App") Verification Service in Android 4.2". Xuxian Jiang. December 2012. URL: http://www.cs.ncsu.edu/faculty/jiang/appverify/
[Ref.- 171]	"Dissecting the Android Bouncer". Jon Oberheide. 2012. URL: https://jon.oberheide.org/files/summercon12-bouncer.pdf
[Ref.- 172]	"Actividad web y de aplicaciones". Google. URL: https://support.google.com/accounts/answer/54068?hl=es
[Ref.- 173]	"Eliminar búsquedas y actividad de navegación". Google. URL: https://support.google.com/accounts/answer/465?hl=es
[Ref.- 174]	"Crear una copia de seguridad de tus fotos y vídeos automáticamente". Google. URL: https://support.google.com/plus/answer/1647509

Referencia	Título, autor y ubicación
[Ref.- 175]	"Función Reconóceme en fotos y vídeos". Google. URL: https://support.google.com/plus/answer/2370300?hl=es
[Ref.- 176]	"Ver fotos en las que te hayan etiquetado". Google. URL: https://support.google.com/plus/answer/1254833?hl=es
[Ref.- 177]	" How to Install and Use the Google Experience Launcher on Any Android Device". How-To-Geek. November 2013. URL: http://www.howtogeek.com/176009/how-to-install-and-use-the-google-experience-launcher-on-any-android-device/
[Ref.- 178]	"New NFC capabilities through Host Card Emulation". Google. URL: http://developer.android.com/about/versions/kitkat.html#44-hce
[Ref.- 179]	"Cómo compartir contenido con Android Beam". Google. URL: https://support.google.com/nexus/answer/2781895?hl=es
[Ref.- 180]	"Utilizar la función Tocar y pagar con tu dispositivo". Google. URL: https://support.google.com/nexus/answer/3470787?hl=es
[Ref.- 181]	"Security Tips". Google. 2015. URL: http://developer.android.com/training/articles/security-tips.html
[Ref.- 182]	"Utilizar certificados". Google. URL: https://support.google.com/nexus/answer/2844832?hl=es
[Ref.- 183]	"ID de publicidad". Google. URL: https://support.google.com/googleplay/android-developer/answer/6048248?hl=es
[Ref.- 184]	"Nexus 5 Stock OTA URLs". XDA Developers. URL: http://forum.xda-developers.com/google-nexus-5/general/ref-nexus-5-stock-ota-urls-t2475327
[Ref.- 185]	"Using the ICS KeyChain API" (4.0, ICS). Nikolay Elenkov. Novemeber 2011. URL: http://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html "ICS Credential Storage Implementation". Part 1 & 2. Novemeber/December 2011. URL: http://nelenkov.blogspot.com.es/2011/11/ics-credential-storage-implementation.html URL: http://nelenkov.blogspot.com.es/2011/12/ics-credential-storage-implementation.html
[Ref.- 186]	"ICS Trust Store Implementation" (4.0, ICS). Nikolay Elenkov. December 2011. URL: http://nelenkov.blogspot.com.es/2011/12/ics-trust-store-implementation.html
[Ref.- 187]	"Certificate blacklisting in Jelly Bean" (4.1, JB). Nikolay Elenkov. July 2012. URL: http://nelenkov.blogspot.com.es/2012/07/certificate-blacklisting-in-jelly-bean.html
[Ref.- 188]	"Jelly Bean hardware-backed credential storage" (4.1, JB). Nikolay Elenkov. July 2012. URL: http://nelenkov.blogspot.jp/2012/07/jelly-bean-hardware-backed-credential.html
[Ref.- 189]	"Questioning the chain of trust: investigations into the root certificates on mobile devices ". Andrew Blaich. Bluebox. October 2014. URL: https://bluebox.com/blog/technical/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/
[Ref.- 190]	"Android User Security Guide". Bluebox. URL: https://bluebox.com/android-user-security-guide/ URL: http://offers.bluebox.com/rs/blueboxsecurity/images/guide-android-user-security.pdf
[Ref.- 191]	"Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". Raúl Siles. DinoSec. February 2015. URL: http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html
[Ref.- 192]	"Is Android 4.4.4 vulnerable to CVE-2014-6060 (DoS in dhcpcd)? ". Android Google Code. Raul Siles. February 2015. URL: https://code.google.com/p/android/issues/detail?id=144663 (*Este enlace podría ser privado y no estar visible en el momento de la publicación de la guía*)
[Ref.- 193]	"Android Internals: A Confectioner's Cookbook". Jonathan Levin. 2015. URL: http://newandroidbook.com URL: http://newandroidbook.com/files/Andevcon-ART.pdf ("ART (& OAT) Internals")